

Management Software

AT-S25



User's Guide

FOR USE WITH AT-8316F/MT, AT-8316F/VF,
AT-8316F/SC, AND AT-8324 FAST ETHERNET
SWITCHES

VERSION 1.4

PN 613-10844-00 Rev C

 Allied Telesyn

Simply Connecting the World

Copyright © 2001 Allied Telesyn International, Corp.
960 Stewart Drive Suite B, Sunnyvale, CA 94085 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn International, Corp.

Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn International, Corp. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn International, Corp. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn International, Corp. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

Preface	7
Supported Platforms	7
Purpose of This Guide	8
How This Guide is Organized	9
Document Conventions	10
Where to Find Related Guides	11
Contacting Allied Telesyn	12
Online Support	12
Technical Support and Services	12
Technical Support E-mail Addresses	12
Returning Products	13
FTP Server	14
For Sales or Corporate Information	15
Tell Us What You Think	16
 Chapter 1	
Getting Started	17
Overview	18
Starting a Local Omega Session	19
Omega Main Menu	20
Selecting Menu Options and Changing Parameters	21
Quitting from a Local Session	23
Starting an Omega Session from a Web Browser	24
Managed Switch	26
Omega Main Menu Window	26
Selecting Menu Options and Changing Parameters	27
Web Links	28
Browser Tools	28
Quitting an Omega Session from a Web Browser	28
Starting a Telnet Management Session	29
Starting an SNMP Management Session	30
Connecting to a Remote Stack	31
Menu Tree	32

Chapter 2

Managing a Stack	37
Configuring IP Parameters	38
Configuring Spanning Tree Protocol Parameters	43
Configuring the Port Parameters	43
Configuring STP Parameters	46
Enabling or Disabling IGMP Snooping	49
Naming a Stack	50
Resetting a Stack	51
Reactivating the Default Settings on a Stack	53
Configuring the RS232 Port on the Master Switch	55
Running Diagnostics	58
Displaying the Activity Monitor	60
Pinging a Device	61

Chapter 3

Configuring the Ports	63
Displaying Port Status	64
Configuring Port Parameters	66
Configuring Port Trunks	70
Guidelines	70
Creating a Port Trunk	73
Deleting a Port Trunk	75
Configuring a Port Mirror	76
Enabling Port Mirroring	76
Disabling Port Mirroring	78
Configuring Port Security	79

Chapter 4

Configuring the MAC Address Table	81
MAC Address Table	82
Displaying the MAC Address Table	83
Displaying the MAC Addresses of a Port	84
Displaying the Port Number of a MAC Address	85
Changing the Aging Time of the MAC Address Table	86
Static MAC Address Table	87
Displaying the Static MAC Address Table	87
Adding Addresses to the Static MAC Address Table	88
Deleting Addresses from the Static MAC Address Table	90
Clearing the Static MAC Address Table	91
Multicast Addresses	92
Configuring a Multicast Address	92
Changing a Multicast Port Assignment	94
Deleting a Multicast Address	94

Chapter 5

Configuring Virtual LANs and Quality of Service	97
Creating a New VLAN	98
Example of Creating a Port-based VLAN	101
Example of Creating a Tagged VLAN	103
Modifying a VLAN	105
Deleting a VLAN	106
Activating or Deactivating the Basic VLAN Mode	107
Configuring Quality of Service	108
Assigning the CPU Management Port to a VLAN	110

Chapter 6

Displaying Ethernet Statistics	113
Displaying Statistics for Received Frames	114
Displaying Statistics for Transmitted Frames	118
Displaying RMON Statistics for a Switch	120
Displaying RMON Statistics for a Port	121
Resetting the Statistics Counters	122
Interpreting the Graphs	123

Chapter 7

Configuring the Omega Interface	125
Creating an Omega Password	126
Specifying a Timeout Value	128
Enabling and Disabling the Access Methods	129

Chapter 8

Upgrading Switch Software and Configuration Files	131
Upgrading the Stack Software	132
Using XModem to Upgrade the Stack Software	133
Using TFTP to Upgrade Software.....	134
Using Omega to Upgrade Additional Stacks	135
Downloading Software to One Stack.....	135
Downloading Software to All Switches.....	136
Uploading and Downloading System Configuration Files	137

Appendix A

Introduction to Virtual LANs	139
Port-based VLAN	141
Parts of a Port-based VLAN.....	141
General Rules to Creating a Port-based VLAN	143
Port-based VLAN Example	144
Drawbacks to Port-based VLANs	146
Tagged VLAN	147
Parts of a Tagged VLAN.....	148
General Rules to Creating a Tagged VLAN	149
Tagged VLAN Example	150
Basic VLAN Mode	152

Appendix B

AT-S25 Default Settings	153
--------------------------------------	-----

Appendix C

Spanning Tree Protocol Concepts	155
Spanning Tree Protocol Features	156
Spanning Tree Protocol Parameters	157
Spanning Tree Protocol Operation	158
Communication Between Bridges	158
Selecting a Root Bridge and Designated Bridges.....	158
Selecting Designated Ports.....	158
Handling Duplicate Paths.....	158
Remapping Network Topology.....	158

Appendix D

Supported Platforms	159
----------------------------------	-----

Index	161
--------------------	-----

Preface

This guide contains instructions on how to use the AT-S25 Fast Ethernet Switch software and the Omega management interface to configure and manage your Allied Telesyn AT-8300 Series Fast Ethernet Switches.

Supported Platforms

Version 1.4 of the AT-S25 software is supported on the following devices:

- ☐ AT-8316F/MT Fast Ethernet Switch
- ☐ AT-8316F/VF Fast Ethernet Switch
- ☐ AT-8316F/SC Fast Ethernet Switch
- ☐ AT-8324 Fast Ethernet Switch
- ☐ AT-STACK8 Stacking Module

This version supports the following optional expansion modules:

- ☐ AT-A14 100/1000Base-T (RJ-45) Expansion Module
- ☐ AT-A15/SX 1000Base-SX (SC) Expansion Module
- ☐ AT-A15/LX 1000Base-LX (SC) Expansion Module
- ☐ AT-A16 100Base-FX (VF-45) Expansion Module
- ☐ AT-A17 100Base-FX (SC) Expansion Module
- ☐ AT-A18 10/100Base-TX (RJ-45) Expansion Module
- ☐ AT-A19 100Base-FX (MT-RJ) Expansion Module

- ❑ AT-A24/SX 1000Base-SX (MT-RJ) Expansion Module
- ❑ AT-A24/LX 1000Base-LX (MT-RJ) Expansion Module

Refer to **Appendix C, Supported Platforms**, for additional information on the switches and optional expansion modules supported by this version of the AT-S25 management software.

Purpose of This Guide

This guide is intended for network administrators who are responsible for managing the switches. Network administrators should be familiar with Ethernet switches, Ethernet and Fast Ethernet technology, bridging, and the Spanning Tree Protocol (STP).

How This Guide is Organized

This guide contains the following chapters and appendices:

Chapter 1, **Getting Started**, explains how to start an Omega management session and how to navigate around the Omega menus.

Chapter 2, **Managing a Stack**, describes how to configure the IP parameters for a stack, how to set the STP parameters, and more.

Chapter 3, **Configuring the Ports**, explains how to set port parameters, create port trunks, and configure a port mirror.

Chapter 4, **Configuring the MAC Address Table**, contains the procedures for displaying the MAC address table, viewing and changing the static MAC address table, and configuring multicast addresses.

Chapter 5, **Configuring Virtual LANs and Quality of Service**, contains the procedures for creating and modifying VLANs in a stack and how to configure the priority queuing for Quality of Service.

Chapter 6, **Displaying Ethernet Statistics**, explains how to use the Omega program to view switch-level and port-level performance statistics.

Chapter 7, **Configuring the Omega Program**, contains the procedures for configuring the security features of the Omega program.

Chapter 8, **Upgrading Switch Software and Configuration Files**, explains how to download new AT-S25 software onto the AT-8324 and AT-8316F Series switches in your network.

Appendix A, **Introduction to Virtual LANs**, describes the different types of VLANs supported by an AT-8300 stack.

Appendix B, **Switch Default Settings**, contains the factory default settings for the switch.

Appendix C, **Spanning Tree Concepts**, briefly describes the Spanning Tree Protocol (STP) as implemented by Allied Telesyn on the switches.

Appendix D, **Supported Platforms**, lists the basic specifications of the switches and optional expansion modules supported by this version of the AT-S25 management software.

Index, at the end of this guide, is organized according to subject matter.

Document Conventions

This guide uses several conventions that you should become familiar with before you begin to perform the procedures.

Note

Notes provide additional information.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Related Guides

The Allied Telesyn web site at www.alliedtelesyn.com contains the most recent documentation and technical information for all of our products. All web-based documentation for this product and other Allied Telesyn products can be downloaded from the web site in PDF format.

For hardware installation instructions for the switch, refer to the following guide:

- ❑ **AT-8316F/MT, AT-8316F/VF, AT-8316F/SC and AT-8324 Installation Guide**, PN 613-10813-00

This manual is available from the Allied Telesyn web site.

The following manual is shipped with the switch and contains an abbreviated version of the installation instructions:

- ❑ **AT-8316F/MT, AT-8316F/VF, AT-8316FXL/SC, and AT-8324 Quick Install Guide**, PN 613-10812-00

Contacting Allied Telesyn

You can contact Allied Telesyn technical support by telephone, fax and e-mail. You can also contact technical support online through our web site.

Online Support

You can request technical support online by filling out the Online Technical Support Form at www.alliedtelesyn.com/forms/support.htm.

Technical Support and Services

Americas

United States, Canada, Mexico, Central America, South America
Tel: 1 (800) 428-4835, option 4
Fax: 1 (503) 639-3176

Asia

Singapore, Taiwan, Thailand, Malaysia, Indonesia, Korea, Philippines, China, India, Hong Kong
Tel: (+65) 3815-612
Fax: (+65) 3833-830

Australia

Australia, New Zealand
Tel: 1 (800) 000-880
Fax: (+61) 2-9438-4966

France

France, Belgium, Luxembourg, The Netherlands, Middle East, Africa
Tel: (+33) 0-1-60-92-15-25
Fax: (+33) 0-1-69-28-37-49

Germany

Germany, Switzerland, Austria, Eastern Europe
Tel: (+49) 30-435-900-126
Fax: (+49) 30-435-70-650

Italy

Italy, Spain, Portugal, Greece, Turkey, Israel
Tel: (+39) 02-41-30-41
Fax: (+39) 02-41-30-42-00

Japan

Tel: (+81) 3-3443-5640
Fax: (+81) 3-3443-2443

United Kingdom

United Kingdom, Denmark, Norway, Sweden, Finland
Tel: (+44) 1-235-442500
Fax: (+44) 1-235-442680

Technical Support E-mail Addresses

United States and Canada

TS1@alliedtelesyn.com

Latin America, Mexico, Puerto Rico, Caribbean, and Virgin Islands

latin_america@alliedtelesyn.com

Returning Products

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesyn without a RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn's Technical Support at one of the following locations:

- ☐ **United States and Canada**
Toll-free: 1-800-428-4835, option 4
Fax: 1-503-639-3716
- ☐ **Europe, Africa, and Middle East**
Tel: +44-1793-501401
Fax: +44-1793-431099
- ☐ **Latin America, Caribbean, and Virgin Islands**
Tel: International code + 425-481-3852
Fax: International code + 425-481-3895
- ☐ **Puerto Rico**
Tel: 1-800-424-5012, ext. 3852 or
Tel: 1-800-424-4284, ext. 3852
- ☐ **Mexico**
Tel: 800-424-5012, ext. 3852
Fax: International code + 425-481-3895
- ☐ **Asia and Southeast Asia**
Tel: +65 381-5612
Fax: +65 383-3830
- ☐ **Australia**
Tel: 1-800-000-880
Fax: 2-9438-4966
- ☐ **New Zealand**
Tel: 0800-45-5782

FTP Server

If you need a new version of management software for an Allied Telesyn device and you know the file name of the program, you can download the software by connecting directly to our FTP server at <ftp://gateway.centre.com>. At login, enter 'anonymous'. Enter your e-mail address for the password as requested by the server at login.

For Sales or Corporate Information

Allied Telesyn International, Corp.
19800 North Creek Parkway, Suite 200
Bothell, WA 98011
Tel: 1 (425) 487-8880
Fax: 1 (425) 489-9191

Allied Telesyn International, Corp.
960 Stewart Drive, Suite B
Sunnyvale, CA 94085
Tel: 1 (800) 424-4284 (USA and Canada)
Fax: 1 (408) 736-0100

Tell Us What You Think

If you have any comments or suggestions on how we might improve this or other Allied Telesyn documents, please fill out the Send Us Feedback Form at www.alliedtelesyn.com/contact/feedbackf.asp.

Chapter 1

Getting Started

This chapter provides an overview of the Omega management interface and contains the procedures for starting a management session on an AT-8300 Series stack. The sections in this chapter include:

- ❑ **Overview** on page 18
- ❑ **Starting a Local Omega Session** on page 19
- ❑ **Starting an Omega Session from a Web Browser** on page 24
- ❑ **Starting a Telnet Management Session** on page 29
- ❑ **Starting an SNMP Management Session** on page 30
- ❑ **Connecting to a Remote Stack** on page 31
- ❑ **Menu Tree** on page 32

Overview

The Omega management interface is a standard part of the AT-S25 management software. This menu-oriented interface simplifies the task of managing an AT-8300 stack. With it, you can configure and manage all of a stack's parameters. For instance, you can create VLANs, view performance statistics, and configure port parameters.

There are three different ways that you can access the Omega management interface to configure and manage an AT-8300 Series stack. They are:

- ☐ Using the RS232 port on the front panel of the master switch in the stack. This is referred to as a local management session.
- ☐ Using a web browser, such as Netscape Navigator.
- ☐ Using Telnet.

You can also manage a stack using a SNMP program, such as HP Overview; however, this method does not use the Omega interface.

The different sections in this chapter contain procedures on how to start an Omega management session for each method. The chapter also describes the Omega Main Menu and how to move through the various menus.

Starting a Local Omega Session

This section contains the procedure for starting a local Omega session. This type of management session involves connecting a terminal to the RS232 port on the master switch of the stack. To start a local Omega session, perform the following procedure:

1. Connect a terminal or PC with a terminal emulator program to the RS232 port on the master switch.

The master switch is the switch assigned the Stack ID value of 1. For information on Stack ID switch settings, refer to the *AT-8316F/MT, AT-8316F/VF, AT-8316F/SC, and AT-8324 Installation Guide*.

Note

Do not connect the terminal to the RS232 port on a slave switch. To start a local management session on a stack, you must connect the terminal to the RS232 port on the master switch.

2. Configure the terminal or terminal emulator program as follows:

- ☐ Baud rate: 9600
- ☐ Data bits: 8
- ☐ Parity: None
- ☐ Stop bits: 1
- ☐ Flow control: None

Note

These are the default settings for the switch's RS232 terminal interface. The settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program. The Omega program allows you to change these values. For instructions, refer to **Configuring the RS232 Port on the Master Switch** on page 55 in Chapter 2.

3. Press the <Return> key.
4. If prompted for a password, enter the password for the Omega interface.

The default is no password. You can later configure a password (described in **Creating an Omega Password** on page 126 in Chapter 7).

The Omega Main Menu is displayed.

Omega Main Menu

Figure 1 illustrates an example of the Omega Main Menu.

```
Allied Telesyn AT-8324 Ethernet Switch: 1.4
Main Menu

Port status and configuration
Ethernet statistics
Administration
System configuration
Traffic/Port Mirroring
Virtual LANs/QoS
Bridging
MAC Address Table
Quit

Or select a module:
> 1 - Switch / Master
  2 - Switch / Slave
  3 - Switch / Slave
  4 - Switch / Slave
```

Figure 1 Omega Main Menu from a Local Session

The Main Menu is divided into two parts. The top of the Main Menu contains the menu selections and the bottom part displays a list of the switches in the stack.

The ">" symbol is used in the Main Menu to indicate the currently selected switch. When you start an Omega session, the default selected switch is the master switch.

Most of the procedures in this guide start by having you select the switch in the stack on which you want to perform the procedure. For example, to display the status of the ports on switch 3, you would first select switch 3 from the bottom of the Main Menu and then choose *Port status and configuration*.

The number of each switch in the menu corresponds to the Stack ID setting on the switch. The Stack ID setting is assigned with the Stack ID switch on the back panel of the switch. For the location of the switch and information on how each switch is assigned a value, refer to the *AT-8316F/MT, AT-8316F/VF, AT-8316F/SC and AT-8324 Installation Guide*.

Note

The master switch of the stack has the number 1. All other switches are slave switches. When instructed by this manual to select the master switch, be sure to select switch number 1.

Selecting Menu Options and Changing Parameters

The table below shows you how to move through and select menu selections if you are using the DEC VT100 or ANSI (the default) terminal configuration:

Table 1 DEC VT100 or ANSI Terminal

When directed to	You must
Select an option	<p>Highlight the option by pressing the Up (↑) or Down (↓) arrow key; then press <Return></p> <p>or</p> <p>Type the first character of the option you want at the prompt and then press <Return>.</p> <p>If two or more options have matching initial characters, type the initial character enough times until the option you want is highlighted; then press <Return>.</p>
Enter information	Type the information and press <Return>.
Return to the previous screen	<p>Select the option that returns you to the previous menu and press <Return></p> <p>or</p> <p>Press <Esc>.</p>

Table 2 explains how to move through and select menu selections if you are using a generic (dumb) terminal.

Table 2 Generic (Dumb) Terminal

When directed	You must
To select an option	<p>Type the first character of the option you want and then press <Return>.</p> <p>If two or more options have matching initial characters, type enough characters for Omega to distinguish your choice from the other options; then press <Return>. To guide you, the characters you must type are in uppercase.</p> <p>For example: Mirroring configuration MAC Address Table</p> <p>If options on a list are preceded by numbers (1:, 2:, 3:, etc.), type the number corresponding to your choice at the prompt; then press <Return>.</p>
To enter information	Type the information at the prompt and press <Return>.
To return to the previous screen	Press <Return> after making an entry.

Activated options in menus are preceded by a > symbol. In the following example, the first option is activated:

```
> Enable this port
  Disable this port
```

When you press <Return> to select a field in which you can enter a value, the -> symbol is displayed. For example:

```
System name: ->
```

The -> symbol indicates that you can enter a value for the parameter or change the existing value. Once you have entered a value, press <Return>. To delete an existing value to a parameter without assigning a new value, type a space and press <Return>. In most cases, a change to a parameter is activated on the switch immediately.

Quitting from a Local Session

To quit a local Omega session, select *Quit* from the Omega Main Menu. You should always be sure to exit from a management session when you are finished managing a stack. This will prevent unauthorized individuals from making changes to a stack's configuration should you leave your management station unattended.

It should also be noted that you cannot operate both a Telnet management session and a local management session on a stack at the same time. The AT-S25 management software will allow only one Telnet or local session on a stack at a time. Failure to properly exit from a local management session might block you from later accessing the stack with a Telnet utility.

Starting an Omega Session from a Web Browser

This section explains how to start an Omega session from a web browser.

Note

An AT-8300 stack must have an IP address and subnet mask for you to manage it using a web browser. Initially assigning an IP address to a stack can only be performed from a local Omega management session. If you have just install the stack and have yet to assign it an IP address, start a local management session with the stack as explained earlier in this chapter and then assign it an IP address and subnet mask by performing the procedure **Configuring IP Parameters** on page 38 in Chapter 2.

Note

You cannot use a web browser to manage an AT-8300 stack that is a part of a non-TCP/IP network.

To start an Omega session using a web browser, perform the following procedure:

1. Start your web browser.

Note

If your PC with the web browser is connected directly to the stack or is on the same side of a firewall as the stack, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's IP address not to use proxies.

2. Enter the IP address of the stack you want to manage in the URL field of the browser, as shown in Figure 2.

Switch's IP Address



Figure 2 Entering a Switch's IP Address in the URL Field

3. If prompted for a user name and password, enter "admin" for the user name and enter the Omega password in the Password field.

The user name and password prompt appears only if a password has been assigned to the Omega interface. To configure a password, refer to **Creating an Omega Password** on page 126 in Chapter 7. You cannot change the Omega user name.

The window shown in Figure 3 is displayed:

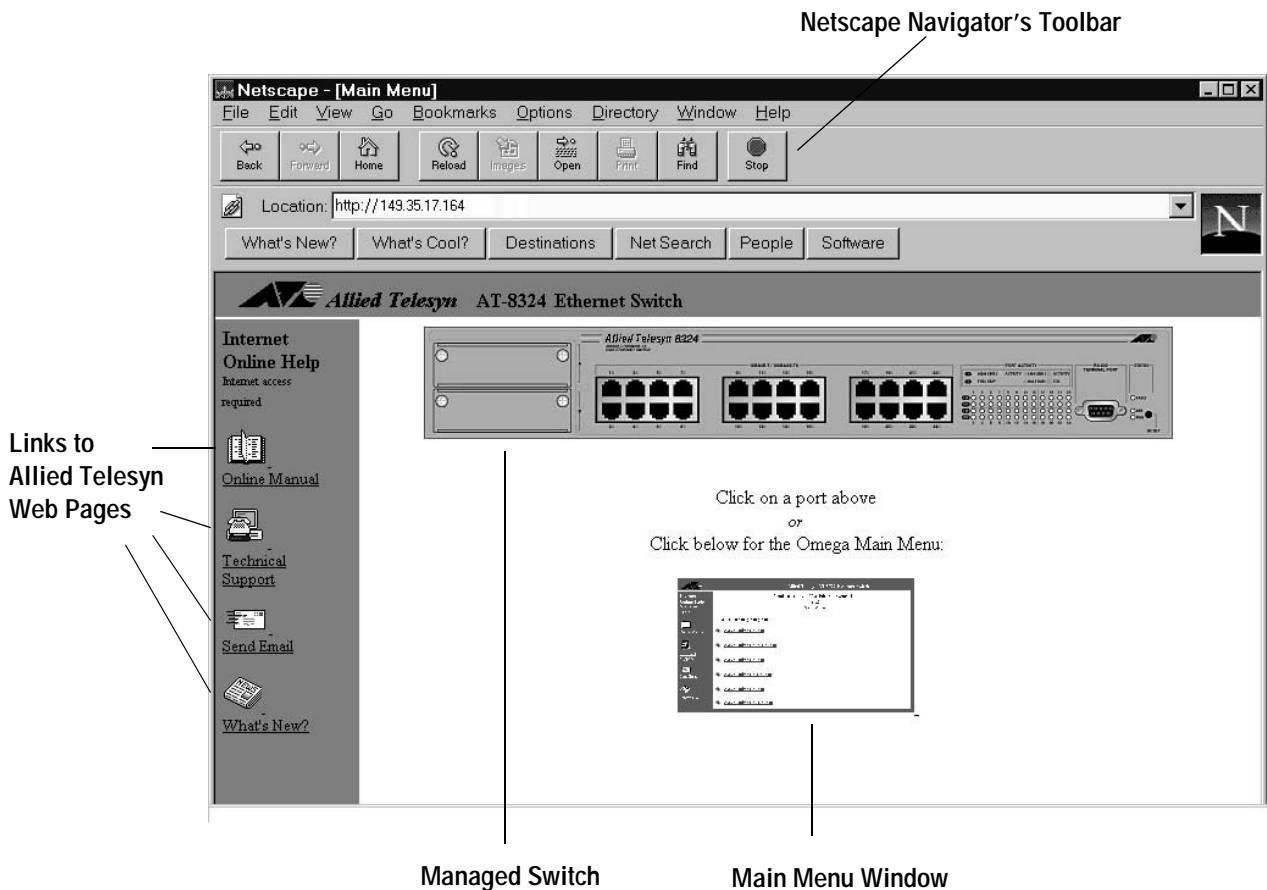


Figure 3 Initial Omega Window from a Web Browser

This window contains the following sections:

- ☐ Managed Switch
- ☐ Main Menu Window
- ☐ Web Links

Managed Switch

At the top of the window is an image of the switch that you are currently managing. This will be an AT-8316F or AT-8324 switch. (The display will not include any expansion modules that might be installed in the switch.)

You can click on certain areas of the image to activate windows. Clicking on a port displays the configuration window for the port, which you use to set the port parameters. Clicking on the RS232 port displays the configuration window for the management port. Finally, clicking on the switch chassis displays a window that lists the status of the ports on the switch.

Omega Main Menu Window

The Main Menu Window contains the Omega menus. This window is displayed in a reduced format when you first start an Omega session from a web browser. To enlarge it, click on the window. Figure 4 illustrates the Omega Main Menu:

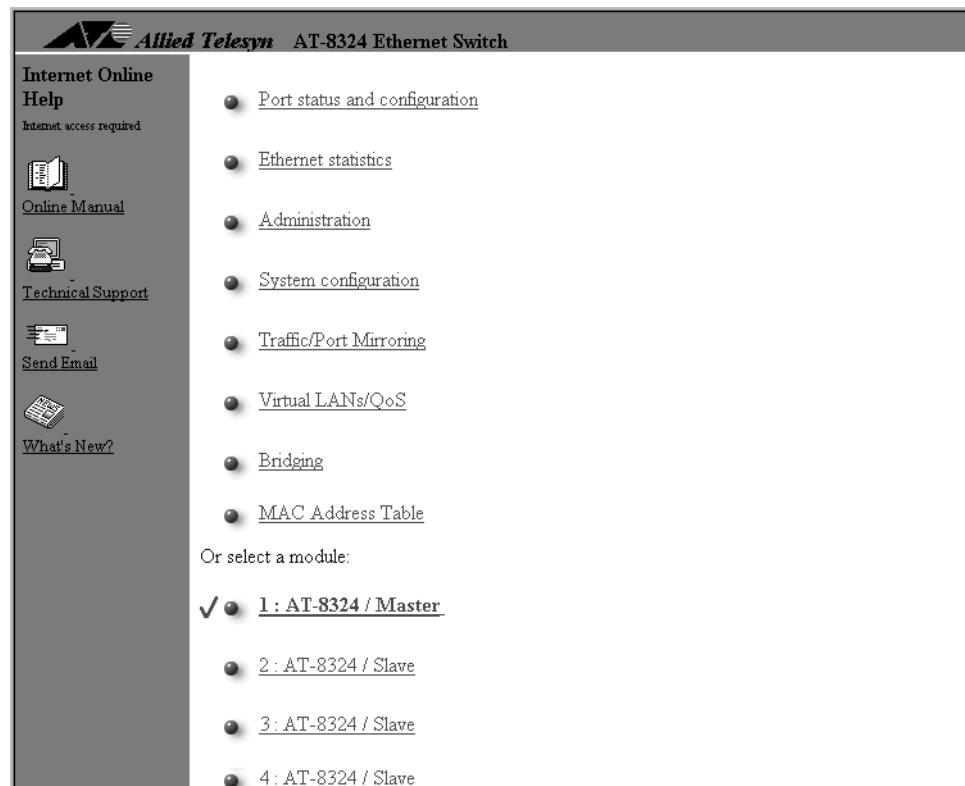


Figure 4 Omega Main Menu from a Web Browser

The Main Menu is divided into two parts. The top of the Main Menu contains the menu selections while the bottom part contains a list of the switches in the stack.

The ✓ symbol is used in the Main Menu to indicate the currently selected switch. When you start an Omega session, the master switch is the selected switch by default.

Most of the procedures in this guide start by having you select the switch in the stack on which you want to perform the procedure. For example, to display the status of the ports on switch 3, you would first select switch 3 from the bottom of the Main Menu and then choose *Port status and configuration*.

The number of each switch in the menu corresponds to the Stack ID setting on the switch. The Stack ID setting is assigned with the Stack ID switch on the back panel of the switch. For the location of the switch and information on how each switch is assigned a value, refer to the *AT-8316F/MT, AT-8316F/VF, AT-8316F/SC and AT-8324 Installation Guide*.

Note

The master switch of the stack has the number 1. All other switches are slave switches. When instructed by this manual to select the master switch, be sure to select switch number 1.

Selecting Menu Options and Changing Parameters

Activated options in the menus are preceded by the ✓ symbol. In the following example, the first option is activated:

- ✓ ☒ [Enable Spanning Tree](#)
- ☐ [Disable Spanning Tree](#)

Figure 5 Active Menu Option

Options in which you can provide a value contain an entry field and the two buttons Enter and Reset, as shown in the following example:

Port name

Figure 6 Entry Field

After entering a new value, press <Return> or click Enter to activate the new parameter setting on the switch. Changes to parameters are activated immediately on the switch.

The Reset button queries the switch for the current parameter setting and displays the setting in the entry field.

Web Links

The left portion of the window contains links that take you automatically to relevant web pages at the Allied Telesyn web site.

The **Online Manual** link takes you to Allied Telesyn's technical communications web page, where you can download product documentation in PDF format.

The **Technical Support** link takes you to Allied Telesyn's Technical Support web page, where you can learn about the company's support services.

The **Send Email** link allows you to submit feedback, questions, or any other information to Allied Telesyn.

The **What's New?** link takes you to a web page that describes Allied Telesyn's latest product offerings.

Browser Tools

You can use the browser tools to move around the Omega menus. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature on frequently-used Omega menus and windows.

Quitting an Omega Session from a Web Browser

To exit from a web-based Omega session, simply quit the browser. It should be remembered that once you have started an Omega session through a browser, the session remains active even if you link to other sites. You can return to the Omega web pages anytime as long as you do not quit the browser.

Starting a Telnet Management Session

To start a Telnet management session, specify the IP address of the AT-8300 Series stack with a Telnet utility. You then enter the Omega password, if one has been assigned, after which the Omega Main Menu is displayed, as shown in Figure 1 on page 20. For instructions on using the Telnet utility, refer to the documentation included with the utility.

Note

An AT-8300 Series stack must have an IP address and subnet mask for you to be able to manage it using a Telnet utility. Initially assigning an IP address to a stack can only be performed from a local Omega management session. If you have just install the stack and have yet to assign it an IP address and subnet mask, start a local management session with the stack as explained earlier in this chapter and then assign it an IP address by performing the procedure **Configuring IP Parameters** on page 38 in Chapter 2.

For non-IP environments, you can use the MAC address assigned to the master switch to connect to the stack, as long as there are no routers between the management station and the stack. The MAC address is printed on a label on the front panel of the switch.

It is important to note that you can have only one Telnet session operating at any one time. The session can be either inbound or outbound. If you have an inbound session to Omega, you do not have the option of starting a new session (outbound connection). Therefore, if you are already using Telnet, the Omega menu selection *Connect to a remote system* will not be available (described in detail in **Connecting to a Remote Stack** on page 31). In addition, a local RS232 connection blocks a Telnet session and vice versa.

If you are currently in a Telnet session, you must disconnect Telnet after quitting Omega. Otherwise, future Telnet or local sessions to the multiplexer will be blocked. You can configure a timeout value so that the management module automatically disconnects a management session after a period of inactivity, as explained in **Specifying a Timeout Value** on page 128 in Chapter 7.

Note

For a description of the Omega main menu, refer to the section **Omega Main Menu** on page 20.

Starting an SNMP Management Session

The final method for managing an AT-8300 Stack from a network management station is by using an SNMP management program, such as HP Openview. This method requires that the switch have an IP address and subnet mask. An SNMP management program will allow you to examine the Management Information Base (MIB) objects on the switch. This method does not employ the AT-S25 management interface. For instructions on using your SNMP program, refer to the documentation that came with the program.

To manage a stack using an SNMP management program, you need to load the stack's MIB file, available from the Allied Telesyn web site, onto the management station. This requires that you use a MIB compiler. To load the MIB file onto a management station, follow the instructions included with your MIB compiler.

Connecting to a Remote Stack

If you are managing a stack locally (that is, through the RS232 port on the master switch), you can connect to another stack through the Omega interface and so be able to manage the remote stack, without having to end your local session. To connect to a remote stack from a local session, perform the following procedure:

1. From the Omega Main Menu, select *Administration*.

The Administrator menu is displayed.

2. Select *Connect to remote system*.
3. Specify the remote stack to be managed using one of the following methods:

- ☐ Stack's IP address, in the format **x.x.x.x**
- ☐ Master switch's MAC address, in the format **xxxxxx xxxxxx**

The switch's MAC address is printed above the switch's RS232 management port on the front panel.

Once the information is validated and the connection to the remote switch is opened, you immediately get the remote switch's Omega Main Menu. You can then use the Omega program to configure or monitor the remote switch.

The only option not available on the remote stack is *Connect to a remote system* from the Administration menu.

4. Select *Quit* from the Main Menu when you are finished managing the remote stack.

After you have ended the session with the remote stack, your Omega session with the local stack is reactivated.

Note

It is important that you select *Quit* after the Omega session. Otherwise, you might block other sessions or software downloads via the network to the remote stack.

Menu Tree

Table 3 lists the menu options in the Omega interface. The table includes a brief function of each selection and the page number of the procedure where the selection is explained.

Table 3 Omega Menu Tree

Main Menu Selection	Menu Selection	Page	Function
Port Status and Configuration			
	Port number	64, 66	Displays and configures the parameter settings for the ports on a switch.
Ethernet Statistics			
	Transmit statistics	118	Displays statistics on the number of frames transmitted by a port or a switch.
	Individual port overview	114, 118	Displays the received and transmitted frame statistics for a specific port.
	RMON statistics	120	Displays RMON statistics for the entire switch.
	Port RMON statistics	121	Displays RMON statistics by port.
	Zero all statistic counters on entire system	122	Returns the statistic counters in a stack to 0 (zero).
Administration			
	Update software in another system	135	Downloads the stack software from one stack to another stack.
	Broadcast updated software to all systems	136	Downloads the stack software from one stack to all the other stacks in the network.
	Xmodem	133	Downloads the AT-S25 software onto the stack. Only available via a local session.

Table 3 Omega Menu Tree (continued)

Main Menu Selection	Menu Selection	Page	Function
	Connect to a remote system	31	Enables you to connect to and manage another stack while running a local management session on a stack. Only available via a local session.
	Ping a remote system	61	Tests the connectivity to another network node.
	Activity monitor	60	Displays the activity monitor for a switch in a stack.
	Diagnostics	58	Performs a series of diagnostic tests on a switch in a stack.
	Reset and restart the system	51	Resets the master switch and all slave switches.
System Configuration			
	System name	50	Assigns a name to a stack.
	Default aging time	86	Sets the aging time for the MAC address table.
	Omega Options	126, 128, 129	Configures the Omega security features, such as the Omega password and timeout value.
	Security / Source Address Table	79	Sets the port security level.
	IP Parameters	38	Configures the IP parameters for the stack, such as the IP address and subnet mask.
	Terminal configuration	55	Adjusts the settings for the RS232 management port on the master switch.
	Port trunking	73, 75	Creates and deletes port trunks.
	Switch-mode selection	107	Enables and disables the Basic VLAN Mode.
	IGMP / No IGMP snooping	49	Enables and disables IGMP snooping on a stack.

Table 3 Omega Menu Tree (continued)

Main Menu Selection	Menu Selection	Page	Function
Traffic/Port Mirroring			
	Enable	76	Enables the port mirroring feature on a switch.
	Disable	78	Disables the port mirroring feature on a switch.
Virtual LANs/QoS			
	Virtual LAN definitions	98, 105, 106	Displays a list of the VLANs existing on a stack. Also creates and deletes virtual LANs.
	Assign port priority	108	Assigns frames to one of two priority queues.
	Assign management port to VLAN	110	Assigns the CPU management port to a VLAN.
Bridging			
	Spanning tree parameters	46	Configures the spanning tree parameters for a stack.
	Port spanning tree configuration	43	Configures the spanning tree parameters for the individual ports on a switch.
MAC Address Table			
	Show all MAC addresses	83	Displays all the MAC addresses learned by the ports on a switch.
	By port MAC addresses	84	Displays the MAC addresses learned on a particular port on a switch.
	Get port from MAC address	85	Displays the port number on which a specific MAC address was learned.
	All static MAC addresses	87	Displays all the entries in the static MAC address table of a switch.
	Per port static MAC address	88, 90	Adds and deletes addresses from the static MAC address table.
	Multicast addresses	92, 94	Displays the multicast addresses of a switch. Also creates and deletes multicast addresses.

Table 3 Omega Menu Tree (continued)

Main Menu Selection	Menu Selection	Page	Function
	Clear static MAC table	91	Clears all entries from the static MAC address table.

Chapter 2

Managing a Stack

The procedures in this chapter show you how to activate and configure many of an AT-8300 stack's parameters. The procedures are as follows:

- ❑ **Configuring IP Parameters** on page 38
- ❑ **Configuring Spanning Tree Protocol Parameters** on page 43
- ❑ **Enabling or Disabling IGMP Snooping** on page 49
- ❑ **Naming a Stack** on page 50
- ❑ **Running Diagnostics** on page 58
- ❑ **Resetting a Stack** on page 51
- ❑ **Configuring the RS232 Port on the Master Switch** on page 55
- ❑ **Reactivating the Default Settings on a Stack** on page 53
- ❑ **Pinging a Device** on page 61
- ❑ **Displaying the Activity Monitor** on page 60

Configuring IP Parameters

If the AT-8300 stack is in a TCP/IP network and you want to manage the stack remotely with a Telnet utility or a web browser, you must assign the stack a set of IP parameters, including a unique IP address and a subnet mask. You can assign these parameters either one of two ways:

- ☐ Manually using the Omega interface
- ☐ Automatically using a BootP or DHCP server.

If you have a BootP or DHCP server on your network, the stack can automatically obtain its IP parameters from the server during startups. In this case, you simply connect the stack to the network. The function of the BootP or DHCP utility within an IP server is to provide IP parameters, including an IP address, to the switches and stacks in the network. Whenever you reset or power cycle an AT-8300 stack, the master switch in the stack transmits a request packet to the server every three seconds to obtain the required IP parameters.

If the master switch receives a response from the BootP or DHCP server, the switch extracts the IP address, subnet mask, and gateway/router address and uses these parameters to configure the stack until the next power-on or reset. Additionally, if the BootP response packet specifies a filename and a server address, then the master switch sends a request to the server using the specified filename. This initiates a download of the operating software and allows you to maintain the downloaded software on your server.

Note

If you have a BootP or DHCP server, the server will provide the IP configuration to the master switch in a stack as long as you configure the server with the master switch's MAC address.

To set the IP parameters for a stack, perform the following procedure:

1. From the Main Menu, select any switch in the stack.

Note

You do not need to select the master switch to set the IP parameters. The parameters, once set, will apply to all switches in the stack.

2. From the Main Menu, select *System Configuration*.

The System Configuration menu shown in Figure 7 is displayed.

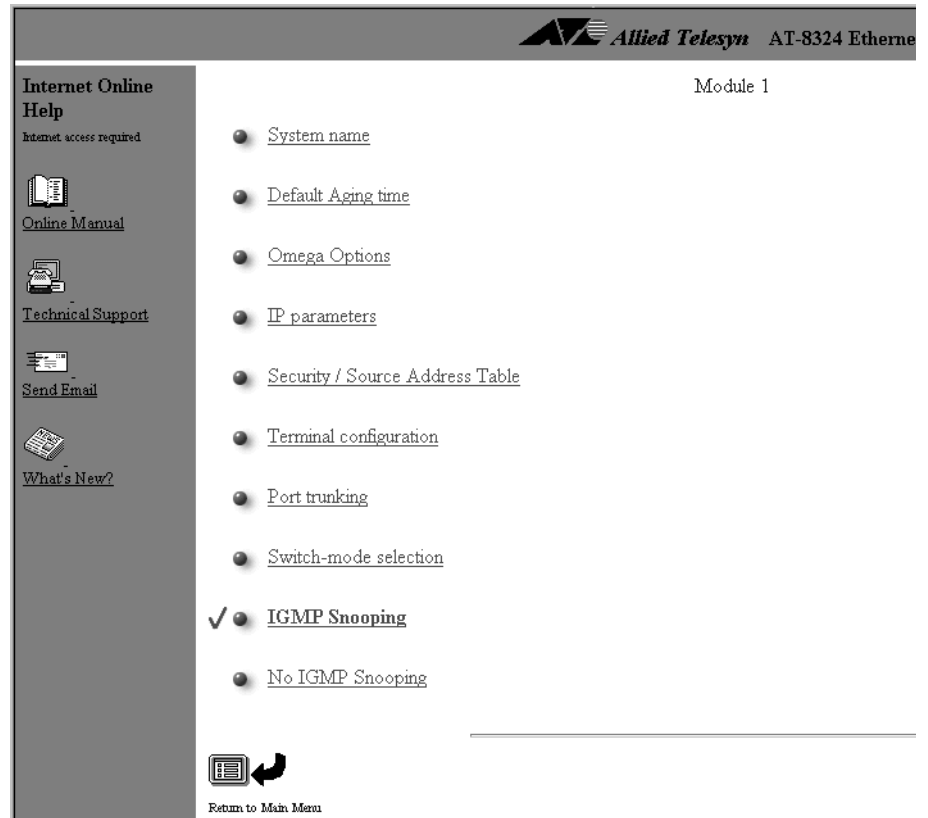
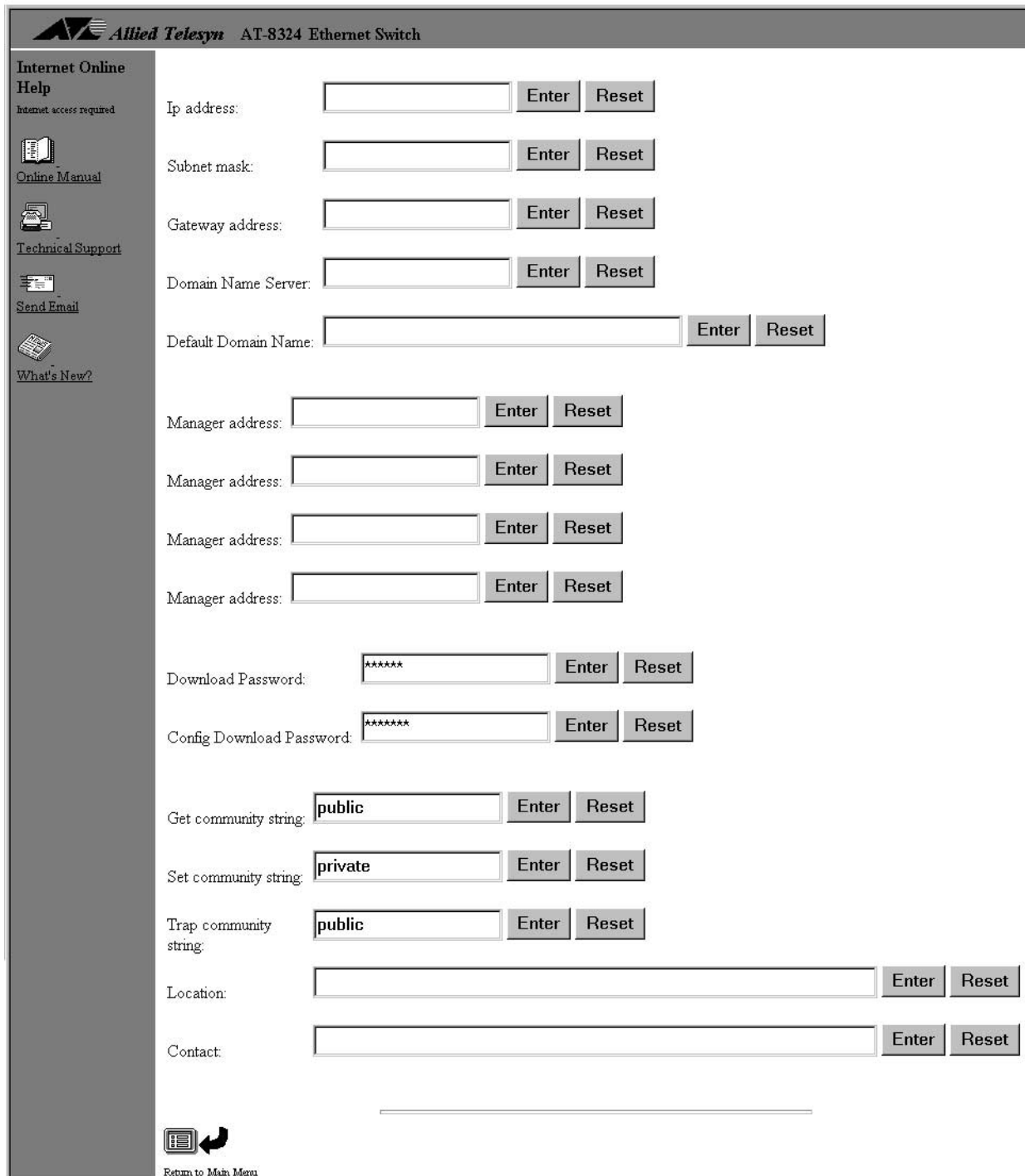


Figure 7 System Configuration Menu

3. Select *IP Parameters*.

The IP Parameters window in Figure 8 is displayed.



The image shows the IP Parameters configuration window for an Allied Telesyn AT-8324 Ethernet Switch. The window has a dark grey header with the Allied Telesyn logo and the device name. On the left is a vertical sidebar with navigation links. The main area contains various configuration fields, each with an 'Enter' and 'Reset' button. The fields include IP address, Subnet mask, Gateway address, Domain Name Server, Default Domain Name, four Manager addresses, Download Password, Config Download Password, Get community string (set to 'public'), Set community string (set to 'private'), Trap community string (set to 'public'), Location, and Contact. A 'Return to Main Menu' button is at the bottom left.

Allied Telesyn AT-8324 Ethernet Switch

Internet Online Help
Internet access required

[Online Manual](#)

[Technical Support](#)

[Send Email](#)

[What's New?](#)

Ip address:

Subnet mask:

Gateway address:

Domain Name Server:

Default Domain Name:

Manager address:

Manager address:

Manager address:

Manager address:

Download Password:

Config Download Password:

Get community string:

Set community string:

Trap community string:

Location:

Contact:


 [Return to Main Menu](#)

Figure 8 IP Parameters Window

4. Enter or change the parameters as desired. Changes to a parameter take effect immediately on the stack.

The parameters in the IP Parameters window are described below:

IP address

This parameter specifies the IP address of the stack. You must specify an IP address if you intend to remotely manage the stack using a web browser, a Telnet utility, or an SNMP management program. If you leave this field blank, the stack will attempt to obtain its IP parameters from a Bootp or DHCP server on the network.

Subnet mask

This parameter specifies the subnet mask for the stack. You must specify a subnet mask if you intend to manage the stack remotely using a web browser, a Telnet utility, or an SNMP management program.

Gateway address

This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the stack from a management station that is separated from the stack by a router.

Domain name server

This is the IP address of the Domain Name Service (DNS). This address is required if you are using this service.

Default domain name

This is the domain name to which the switch belongs. This is recommended if you are using DNS.

Manager addresses

You can enter up to four IP addresses of network management stations or servers that are to receive SNMP traps from the switch. These parameters are optional.

Download password

This password is required when downloading AT-S25 image files from one AT-8300 stack to another stack. The default password is **ATS25**, displayed as a series of asterisks. You can keep the default or change it. A stack can only accept software downloads from another stack of the same product series if their download passwords are the same. The software automatically searches for this password during downloads without requiring you to enter it.

This password is used as the destination filename when you are using TFTP to update the firmware. This password is different from the Omega password that you can create to prevent unauthorized individuals from using the Omega interface to change a stack's configuration settings.

For instructions on how to download the AT-S25 firmware onto a stack, refer to **Chapter 8, Upgrading Switch Software and Configuration Files** on page 131.

Config download password

This password is used when downloading configuration files from one AT-8300 stack to another stack. The default password is config (all lowercase). The Omega interface displays the password as a series of asterisks. For instructions on how to download a configuration file onto a stack, refer to **Chapter 8, Upgrading Switch Software and Configuration Files** on page 131.

SNMP community strings

The following default community strings are provided:

Get - public

Set - private

Trap - public

Location

You can enter a text string to indicate the physical location of the stack (for example, **First Floor, Lab.**) This value is optional.

Contact

You can enter a text string to indicate the name, phone number, and other information to help identify the person responsible for managing the stack. This parameter is optional.

5. After you have set the parameters, return to the Main Menu.

Configuring Spanning Tree Protocol Parameters

The Spanning Tree Protocol (STP) prevents data loops when multiple or redundant paths exist in extended LANs.

Each switch or bridge in a spanning tree domain will:

- ☐ Determine the best single route to a destination device.
- ☐ Update other bridges with topology information by periodically sending Bridge Protocol Data Units (BPDUs).

Once the STP parameters have been configured, bridges can make a determination on the best single path to a destination within a given LAN. A formula determines the amount of time it takes for the topology to reconfigure, depending upon the spanning tree values you use. Refer to the IEEE specification for details.

Most users generally keep the default STP parameters to allow bridges to reconfigure themselves automatically if the topology changes or if bridges become disabled.

For a brief overview of STP, go to **Appendix B, Spanning Tree Concepts**.



Caution

STP on a switch is disabled by default. If you enable STP, the switch provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network.

Configuring the Port Parameters

The Omega program allows you to enable or disable STP on a per port basis and to adjust the STP parameters for each port. To activate and configure the protocol parameters for the individual ports on a switch, perform the following procedure:

1. From the Main Menu, select the switch containing the port or ports to be configured.
2. From the Main Menu, select *Bridging*.

The Bridging menu in Figure 9 is displayed.

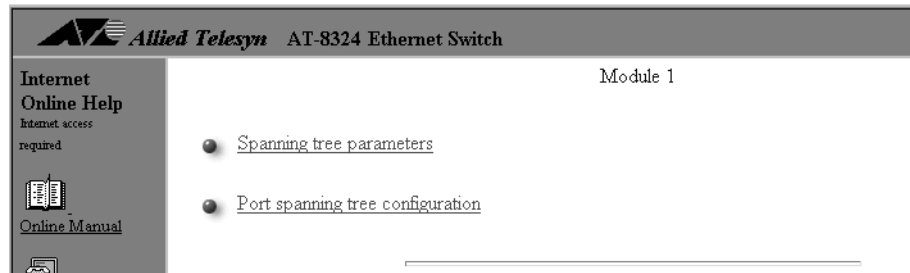


Figure 9 Bridging Menu

3. Select *Port spanning tree configuration*.

The Port Parameters for the Spanning Tree Protocol window in Figure 10 is displayed. The window lists the ports on the switch and the current STP parameter settings for the ports. Figure 10 is an example of the window.

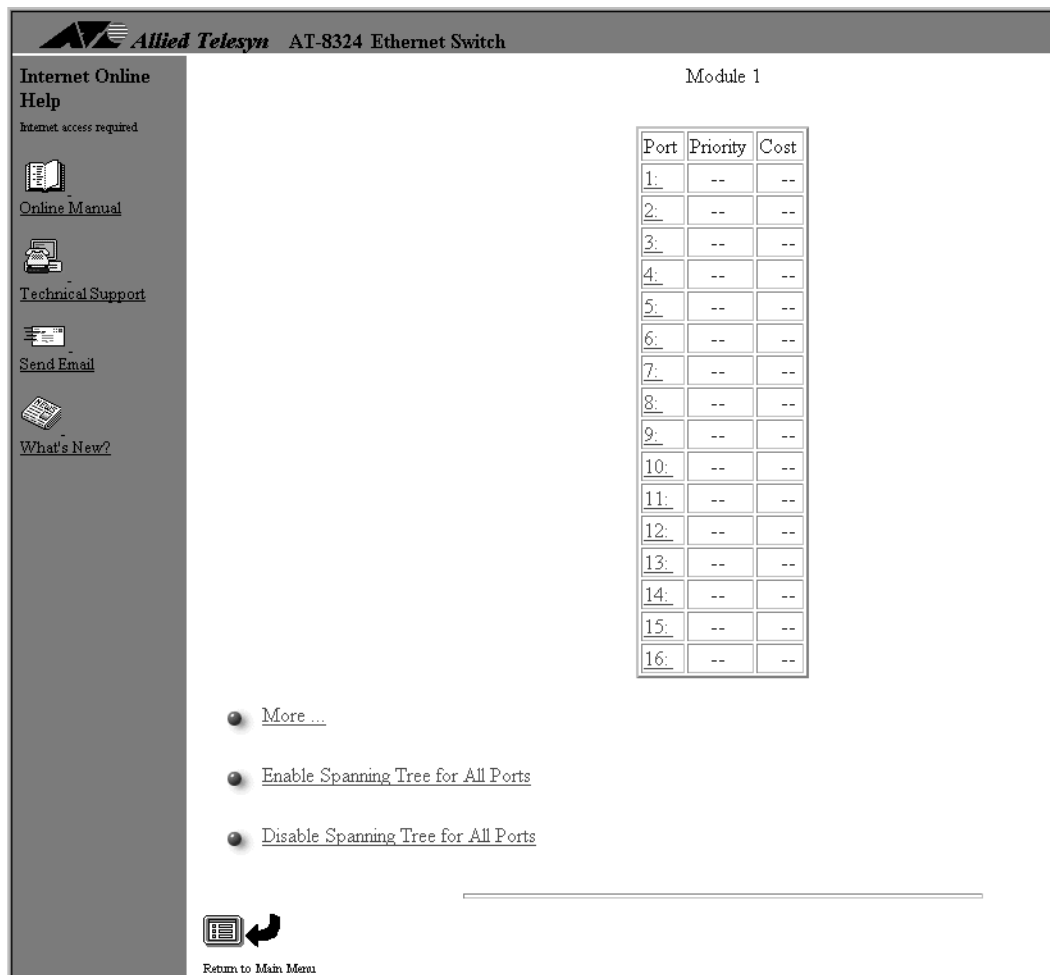


Figure 10 Port Parameters for the Spanning Tree Protocol

4. To enable or disable STP for all the ports on the switch, select either *Enable Spanning Tree for all Ports* or *Disable Spanning Tree for all Ports*.

If you enable STP, the Omega interface sets the port priority to the default value of 128 for each port. For port cost, the default values are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 1 for a 1 Gbps port.

5. To enable or disable STP for a particular port or to change the STP port values, select the port.

The STP Port Parameters window in Figure 11 is displayed.

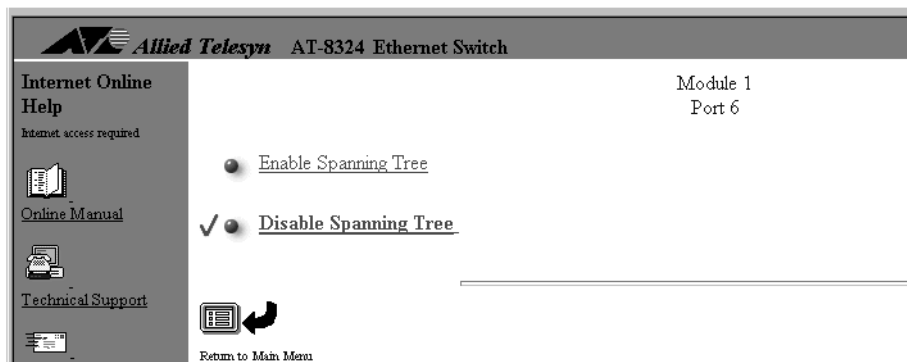


Figure 11 STP Port Parameters Window

If STP is already activated on the port, the port's STP parameters are also displayed, as shown in Figure 12.

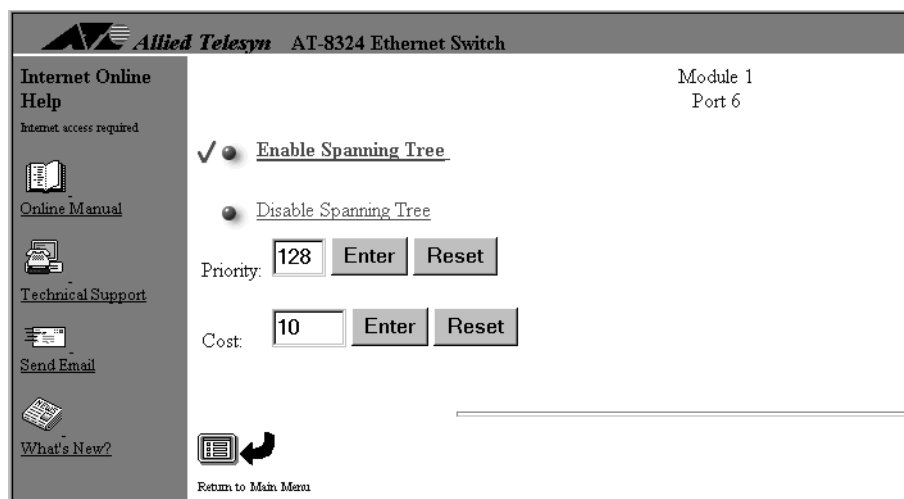


Figure 12 Setting Port STP Parameters Window

6. To enable STP on the port, select *Enable Spanning Tree*. To disable STP on the port, select *Disable Spanning Tree*. If you enable STP, the STP parameters for the port are displayed.

7. Change the priority and port cost parameters for the ports, as desired. The parameters are defined below:

Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The default value for priority is 128. The range is 0-255.

Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The default values for this parameter are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 1 for a 1 Gbps port. The range is 1 to 65535.

8. Return to the Main Menu.

Configuring STP Parameters

This section explains how to set the following STP parameters:

- ☐ Bridge priority
- ☐ Maximum age time
- ☐ Hello time
- ☐ Forwarding delay

To configure these STP parameters for a stack, perform the following procedure:

1. From the Main Menu, select any switch in the stack.

Note

You do not need to select the master switch to set the STP parameters. Once set, the values will apply to all switches in the stack.

2. From the Main Menu, select *Bridging*.

The Bridging menu in Figure 9 on page 44 is displayed.

3. Select *Spanning tree parameters*.

The Spanning Tree Parameters window in Figure 13 is displayed.

Allied Telesyn AT-8324 Ethernet Switch

Internet Online Help
Internet access required

[Online Manual](#)

[Technical Support](#)

[Send Email](#)

[What's New?](#)

Bridge Identifier (Mac Address : Priority) 00a0d5 830f3a : 32768
 Root Bridge Identifier (Mac Address : Priority) 00a0d5 830f3a : 32768
 Cost to the Root 0
 Port closest to the Root 0
 Max Age 20
 Forwarding Delay 15

Bridge Priority:

Max age time:

Hello time:

Forwarding delay:

[Return to Main Menu](#)

Figure 13 Spanning Tree Parameters Window

4. Adjust the settings as desired.

The parameters are discussed below.

Bridge Priority

Bridges use this number to determine the root bridge for a loop-free implementation. If bridges happen to have equal priority values, the bridge with the numerically lowest MAC address becomes the root bridge. When the root bridge malfunctions, the bridge with the next priority number (or the next lowest MAC address) automatically takes over as root bridge. This parameter can be from 0 (zero) to 65,535, with 0 being the highest priority.

Max Age Time

All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). This parameter can be from 6 to 40 seconds. The default is 20 seconds. For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds.

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

Hello Time

Bridges use this parameter to determine the time interval between generating and sending configuration messages. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Forwarding Delay

This parameter indicates the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change; therefore, loops may result. The default is 15 seconds.



Caution

You should consult the IEEE 802.1d standard before changing the Max Age Time, the Hello Time, and the Forwarding Delay parameters.

5. Return to the Main Menu.

Enabling or Disabling IGMP Snooping

An AT-8300 stack supports the Internet Group Management Protocol (IGMP) snooping feature. This feature allows the stack to take advantage of performance improvements provided by IP multicasting. Allied Telesyn's implementation supports IGMP Version 1.

A stack uses IGMP snooping to obtain information about multicast groups by looking at IGMP packets sent from hosts and routers, and also by looking at Distance Vector Multicast Routing Protocol (DVMRP) packets. IGMP packets provide information about nodes joining multicast groups, while DVMRP packets provide information about delivery paths. With this information, the stack builds membership groups of ports for each IP multicast address.

To enable or disable IGMP snooping in a stack, perform the following procedure:

1. From the Main Menu, select any switch in the stack.

Note

You do not need to select the master switch to enable or disable IGMP snooping in a stack. A change to the IGMP setting applies to all switches in a stack.

2. From the Main Menu, select *System configuration*.

The following options in the System Configuration menu are used to enable or disable IGMP snooping.

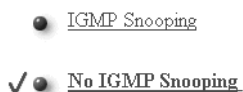


Figure 14 IGMP Snooping Options

3. Toggle the options to enable or disable IGMP snooping.
4. Return to the Main Menu.

Naming a Stack

This procedure assigns a name to a stack. The name is displayed in all the Omega windows when you manage the stack.

To assign a name to a stack, perform the following procedure:

1. From the Main Menu, select any switch in the stack.

Note

You do not need to select the master switch to assign a name to a stack. Once assigned, a name will apply to all switches in the stack.

2. From the Main Menu, select *System Configuration*.

The System Configuration menu in Figure 7 on page 39 is displayed.

3. Select *System Name*.

The prompt in Figure 15 is displayed.

System name



Return to Main Menu

Figure 15 System Name Prompt

4. Enter a unique name of up to 20 characters in the type-in field. Select Enter. The stack's name must be unique within the subnet.

The new name will appear at the top of the screen and will be displayed in every Omega screen from now on.

5. If the stack already has a name that you want to delete without entering a new name, do one of the following:

From a web-based Omega session, delete the existing name and press <Return> or select Enter.

From a local or Telnet Omega session, enter a space in the System name field and press <Return>.

6. Return to the Main Menu.

Resetting a Stack

You might occasionally need to reset the stack. For example, you might need to reset a stack to fix an error condition, to download software through a modem, or to reset all statistics counters to 0 (zero).

You can reset a stack three ways:

- ☐ Pressing the Reset button on the front panel of the switches.
- ☐ Using Omega's Reset and restart option. This option enables you to perform a software reset from a local terminal, a remote location via Telnet, or a web browser.
- ☐ Unplugging the power cords from the power source and plugging them back in to recycle power and reset the switches.

Note

If you reset a stack using the Reset buttons or by unplugging the power cords, you must reset the slave switches first, preferably starting with the slave switch with the highest switch ID, and then the master switch. You cannot reset an individual switch in a stack. You must reset the entire stack.

Note

The following procedure resets the entire stack. You cannot reset one switch in a stack.

To reset a stack using the Omega interface, perform the following procedure:

1. From the Main Menu, select the master switch.

Note

You must select the master switch to perform this procedure. Do not select a slave switch.

2. From the Main Menu, select *Administration*.

The Administration menu in Figure 16 is displayed.

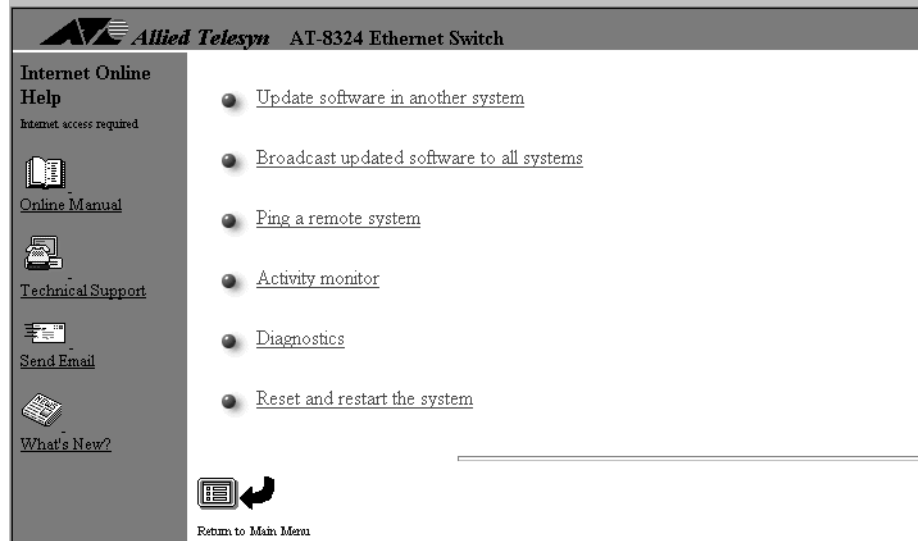


Figure 16 Administration menu

Note

If you are running a local management session, the Administrator menu will contain two additional selections: *XModem software update to this system* and *Connect to a remote system*.

3. Select *Reset and restart the system*.

The master switch will reset itself and the slave switches in the stack. Each switch runs a series of self-tests, which take a few seconds to complete. During the tests, the Fault LED on the front of the switches will flash. Once the tests are completed, the Fault LED will remain OFF.

The master switch begins a discovery process of the stack topology, during which the number and types of switches that constitute the stack are determined. This discovery process takes approximately thirty seconds to complete. Once the discovery process has been completed, the stack will begin to forward packets.

Reactivating the Default Settings on a Stack

This procedure explains how to reset the stack settings to the factory default settings, which are listed in **Appendix A** on page 139. This procedure can only be performed locally through the RS232 port on the master switch.



Warning

This procedure should be performed with caution. Resetting a stack to its default setting deletes all existing settings, including the stack's IP address and port settings. Any defined VLANs also are deleted and all ports are assigned to the Default VLAN.

To reset the stack settings to the factory default settings, perform the following procedure:

1. Attach a terminal or a PC with a terminal emulation program to the RS232 port on the front panel of the master switch.

Note

Do not connect the terminal or PC to a slave switch. You must connect the device to the master switch.

2. Configure the terminal or terminal emulator program as follows:

- ☐ Baud rate: 9600
- ☐ Data bits: 8
- ☐ Parity: None
- ☐ Stop bits: 1
- ☐ Flow control: None

Note

These are the default settings for the RS232 terminal interface. These parameters are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulation program. The Omega program allows you to change these values. For instructions, refer to **Configuring the RS232 Port on the Master Switch** on page 55.

3. Press the Return key.
4. Press the Reset button on the master switch.

5. Immediately press any key when you see the following prompt:

```
Hit any key to run diagnostics or to reload
system software.
```

A menu is displayed.

6. Select D from the menu. The following warning message displays:

```
WARNING: This will erase all current
configuration data!
```

```
Continue? Y/N
```

7. Type Y for yes.

The system displays the following prompt:

```
All configuration data has been reset to
factory default values.
```

8. Type B to boot the stack software.

The master switch will reset itself and run a series of self-tests, which take a few seconds to complete. During the tests, the Fault LED on the front of the switch will flash. Once the tests are completed, the Fault LED will remain OFF.

The master switch begins a discovery process of the stack topology, during which the number and types of switches that constitute the stack are determined. This discovery process takes approximately thirty seconds to complete. Once completed, the stack will begin to forward packets.

Configuring the RS232 Port on the Master Switch

The default settings for the RS232 port on the front panel of the Ethernet switch are as follows:

- ☐ Baud rate: 9600
- ☐ Data bits: 8
- ☐ Stop bits: 1
- ☐ Parity: None
- ☐ Flow control: None

To change the settings for the RS232 port on the master switch, perform the following procedure:

1. From the Main Menu, select the master switch.

Note

You must select the master switch to perform this procedure. Do not select a slave switch.

2. From the Main Menu, select *System Configuration*.

The System Configuration menu in Figure 7 on page 39 is displayed.

3. From the System Configuration menu, select *Terminal Configuration*.

The Terminal Configuration window shown in Figure 17 is displayed.

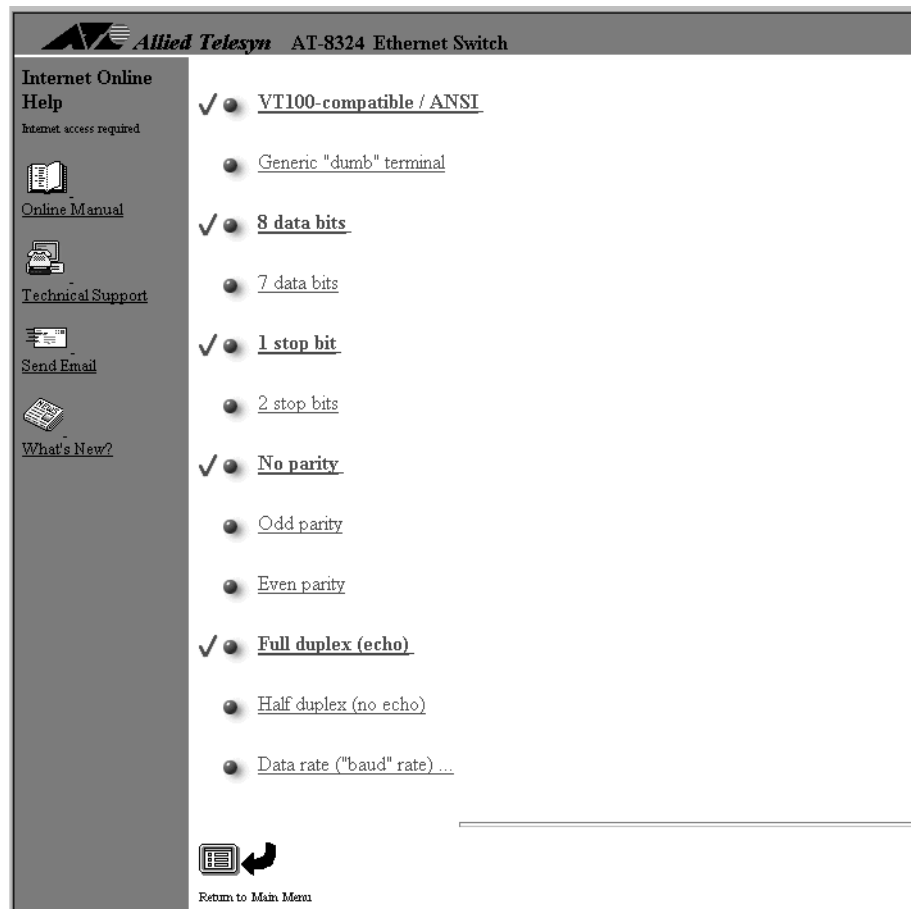


Figure 17 Terminal Configuration Window

If you are running the Omega session from a web browser, you can display the Terminal Configuration window by clicking on the RS232 port in the graphic display of the master switch.

4. Adjust the settings as desired.

The parameters are described below.

VT100-compatible / ANSI

Generic “dumb” terminal

You use these selections to specify the type of terminal. The default is VT100-compatible / ANSI.

8 data bits

7 data bits

These two selections are used to specify the number of data bits. The default is 8 data bits.

1 stop bit**2 stop bits**

These two selections are used to specify the number of stop bits. The default is 1 stop bit.

No parity**Odd parity****Even parity**

These selections are used to specify the parity type. The default is no parity.

Full-duplex (echo)**Half-duplex (no echo)**

These two selections control the duplex mode of the RS232 port. In full duplex, the management module echoes the characters received from the terminal back to the terminal. In half-duplex, the management module does not echo the characters. If each character typed at the terminal is being displayed twice, select the half-duplex mode. The default is full-duplex.

Data rate ("baud" rate)

This selection allows you to specify the speed of the port. When you select this option, the Omega program displays a list of possible baud rates. Possible baud rates are:

- ☐ 19200 bps
- ☐ 9600 bps (recommended setting for fixed baud rate)
- ☐ 4800 bps
- ☐ 2400 bps
- ☐ 1200 bps
- ☐ 600 bps
- ☐ 300 bps
- ☐ 150 bps
- ☐ 75 bps
- ☐ Automatic baud rate detection

The default is Automatic baud rate detection.

5. Return to the Main Menu.

Running Diagnostics

The Omega interface has an option for running diagnostic self-tests on the switches in a stack. The program reports on the operating status of the following switch components:

- ☐ Flash PROM
- ☐ RAM
- ☐ Serial Interface
- ☐ Power supply
- ☐ Operating temperature

The tests also display the following information:

- ☐ AT-S25 version number
- ☐ Stack MAC address
- ☐ Running time

Note

Running the diagnostic tests will not disrupt the network operations of a switch.

To run the self-diagnostics program on a switch in a stack, perform the following procedure:

1. From the Main Menu, select the master or slave switch on which to run the diagnostic tests.
2. From the Main Menu, select *Administration*.
3. From the Administration menu, select *Diagnostics*.

The tests take only a second or two to complete. The results are displayed in the Diagnostics window. An example of the window is shown in Figure 18.

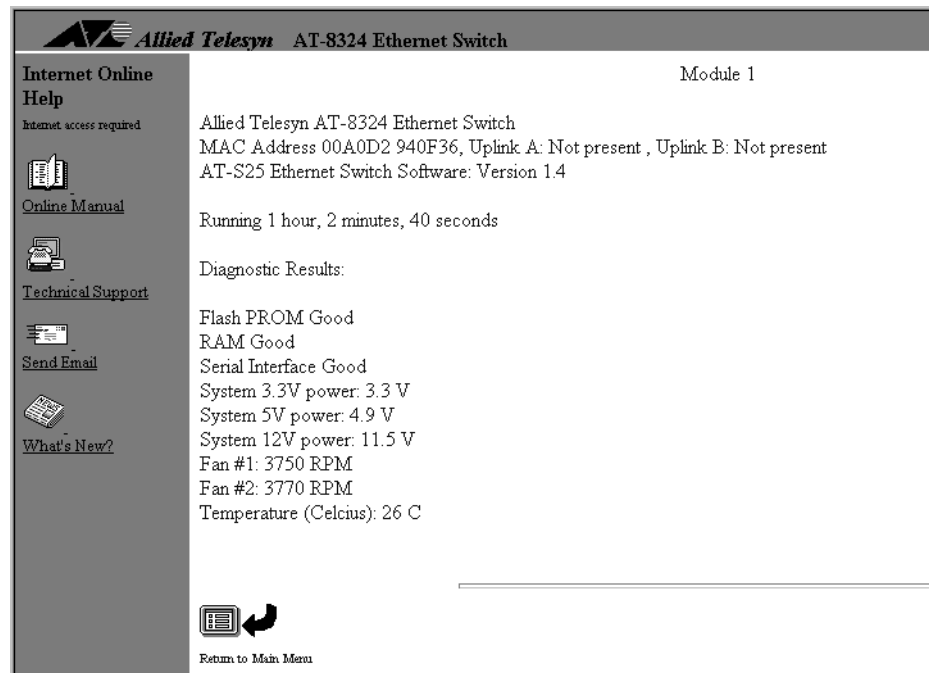


Figure 18 Sample Diagnostics Window

The Flash PROM, RAM, and Serial Interface test results are given as Good or Failed.

Note

The second and third lines in the Diagnostic window, concerning the MAC address, the presence of expansion modules, and the software version number, apply only to the master switch, regardless of the currently selected switch.

4. Return to the Main Menu.

Displaying the Activity Monitor

The Activity Monitor is useful in monitoring the status of a ping command or in determining the status of a software download from switch to switch. To display the Activity Monitor, perform the following procedure:

1. From the Main Menu, select the master switch.
2. From the Main Menu, select *Administration*.
3. From the Administration menu, select *Activity monitor*.

The Activity Monitor window for the stack is displayed. The example shown in Figure 19 displays the results of a ping command.

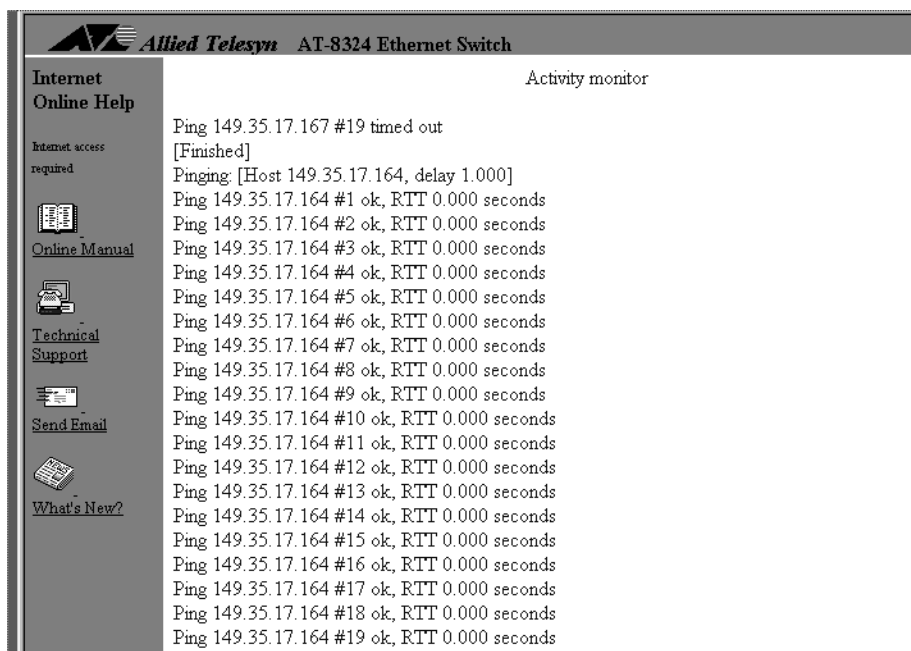


Figure 19 Activity Monitor Window

4. Return to the Main Menu.

Pinging a Device

The ping command allows you to test if an end system can be reached by sending it an Internet Control Message Protocol (ICMP) echo request. If the system is connected to the network and operating, it sends a reply to the requesting system.

To ping another device, perform the following procedure:

1. From the Main Menu, select any switch in the stack.
2. From the Main Menu, select *Administration*.
3. From the Administration menu, select *Ping a remote system*.

The Ping window in Figure 20 is displayed.

Figure 20 Ping Window

4. Specify the device to ping using one of the following methods:
 - ☐ By its IP address in the format **x.x.x.x**
 - ☐ By its MAC address in the format **xxxxxx xxxxxx**

The activity monitor reports the results of the ping command. Figure 21 is an example.

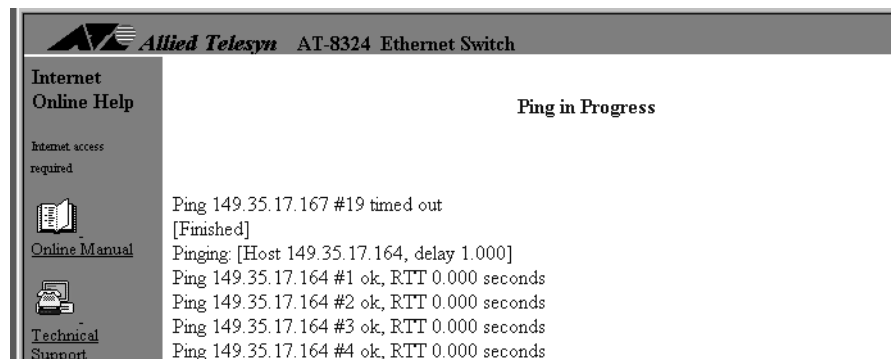


Figure 21 Ping Results Example

Performing a ping command from a web-based Omega session stops after a set number of ping attempts. Performing a ping command from a local or remote Omega session continues until you stop it.

5. Return to the Main Menu.

Chapter 3

Configuring the Ports

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch. Examples of port parameters include duplex mode and, in the case of the AT-8324 switch, port speed. This chapter also describes port trunking and port mirroring.

This chapter contains the following procedures:

- ❑ **Displaying Port Status** on page 64
- ❑ **Configuring Port Parameters** on page 66
- ❑ **Configuring Port Trunks** on page 70
- ❑ **Configuring a Port Mirror** on page 76
- ❑ **Configuring Port Security** on page 79

Displaying Port Status

The Port Status window displays the current operating status of all the ports on a switch in a stack, including any expansion modules, if installed. The window enables you to quickly ascertain the operating status of the ports by displaying a variety of information, such as whether a link exists between the ports and the end nodes, and whether any of the ports have been manually disabled.

To display the status of the ports on a switch, perform the following procedure:

1. From the Main Menu, select the switch whose port status you want to view.
2. From the Main Menu, select *Port Status and Configuration*.

The Port Status window in Figure 22 is displayed.

Internet Online Help
Internet access required

[Online Manual](#)

[Technical Support](#)

[Send Email](#)

[What's New?](#)

Module 1

Port	Link	Status	Mode
1.	Online/10	Enabled	Auto negotiate
2.	Online/10	Enabled	Auto negotiate
3.	Online/10	Enabled	Auto negotiate
4.	Online/10	Enabled	Auto negotiate
5.	Online/10	Enabled	Auto negotiate
6.	Offline	Disabled	Auto negotiate
7.	Online/10	Enabled	Auto negotiate
8.	Online/10	Enabled	Auto negotiate
9.	Online/10	Enabled	Auto negotiate
10.	Online/10	Enabled	Auto negotiate
11.	Online/10	Enabled	Auto negotiate
12.	Online/10	Enabled	Auto negotiate
13.	Online/10	Enabled	Auto negotiate
14.	Online/10	Enabled	Auto negotiate
15.	Online/10	Enabled	Auto negotiate
16.	Online/10	Enabled	Auto negotiate
17.	Online/10	Enabled	Auto negotiate
18.	Online/10	Enabled	Half duplex
19.	Online/10	Enabled	Auto negotiate
20.	Online/10	Enabled	Auto negotiate
21.	Online/10	Enabled	Auto negotiate
22.	Offline	Enabled	Auto negotiate
23.	Offline	Enabled	Auto negotiate
24.	Offline	Enabled	Auto negotiate

Refresh

Figure 22 Port Status Window

The Port Status window contains the following information:

Port

This column displays the number and name of each port. You can assign names to the ports to make them easier to identify. For instructions on assigning port names, refer to **Configuring Port Parameters** on page 66.

The standard twenty four ports on an AT-8324 switch are numbered 1 to 24, and the standard sixteen ports on an AT-8316F switch are numbered 1 to 16.

Link

This column indicates whether there is an active connection between a port and the device connected to the port. Offline indicates that there is no link, while Online indicates that there is a link. If a port is online, this column will also specify the operating speed of the port.

Status

This column indicates whether a port is enabled or disabled. For instructions on how to manually disable or enable a port, refer to **Configuring Port Parameters** on page 66.

Mode

This column indicates the duplex mode of the ports. Possible values are auto-negotiate, full-duplex, or half-duplex. For instructions on how to manually set the duplex mode of a port, refer to **Configuring Port Parameters** on page 66.

The web-based Omega interface features a Refresh button at the bottom of the window. You can use the button to query the switch for the latest port status and displays the status on the screen.

3. Return to the Main Menu.

Configuring Port Parameters

This section contains the procedure for configuring the parameters for the individual ports on a switch.

To view and configure the parameter settings for a port on a switch, perform the following procedure:

1. From the Main Menu, select the switch in the stack with the port to be configured.

2. From the Main Menu, select *Port Status and Configuration*.

The Port Status window in Figure 22 on page 64 is displayed.

3. Select the port to be configured.

The Port Configuration window in Figure 23 is displayed.

Allied Telesyn AT-8324 Ethernet Switch

Internet Online
Help
Internet access required

Module 1
Port 4

[Online Manual](#)

[Technical Support](#)

[Send Email](#)

[What's New?](#)

- ☐ [Receive Statistics Graph](#)
- ☒ [Enable this port](#)
- ☐ [Disable \(partition\) this port](#)
- ☒ [Auto negotiate](#)
- ☐ [Full duplex](#)
- ☐ [Half duplex](#)
- ☐ [Backpressure enabled \(Half Duplex\)](#)
- ☒ [No backpressure](#)
- ☐ [Flow control \(Full Duplex\)](#)
- ☒ [No flow control](#)
- ☐ [Discard broadcast packets](#)
- ☒ [Regular forwarding of broadcasts](#)
- ☐ [Global config](#)

Port name

Figure 23 Port Configuration Window

If you are running the Omega program from a web browser, you can display this window by clicking on a port in the graphical image of the managed switch.

4. Toggle the options as desired.

Any changes to the port settings are activated immediately on the port. The options are described below.

Receive Statistics Graph

This option displays performance statistics for the port, specifically the number and types of frames and errors that have occurred on the port. For further information on port statistics, refer to **Chapter 5, Displaying Ethernet Statistics**.

This option is not available from a local or Telnet management session.

Enable this port

Disable (partition) this port

These selections allow you to manually disable or enable a port in the stack. When a port is disabled, it no longer receives or sends packets. You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. The default is enabled.

Auto-negotiate

Full-duplex

Half-duplex

These three selections control the duplex mode of the port. You can also use these selections on an AT-8324 switch to control port speed.

Full-duplex means that the port can both send and receive data simultaneously. You can select this setting for a port if you know that the device connected to the port supports full-duplex.

Half-duplex means the port can send or receive data, but not both at the same time. Use this setting if you know that the device connected to the port supports half-duplex mode.

Auto-negotiate means that the port negotiates with the connected device to automatically configure to the highest common setting. This setting eliminates the need to reconfigure the port if you change the type of device connected to the port. Both end devices need to be auto-negotiation compliant (802.3u) for the best possible performance settings. If a connected device is not compliant, it should only be configured for half-duplex. Auto-negotiate is the default for all ports.

If the port is on an AT-8324 switch and you select the full-duplex or half-duplex setting rather than the default setting of auto-negotiate, prompts are displayed for the port speed, as shown in Figure 24. The port speed on an AT-8324 switch can be 10 Mbps or 100 Mbps. (The 100 Mbps port speed on an AT-8316F Series switch cannot be changed.)

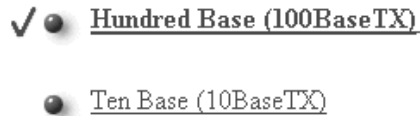


Figure 24 Port Speed Setting for an AT-8324 Switch

Backpressure enabled (half-duplex)

No backpressure

Backpressure applies only to ports operating in half-duplex mode. Backpressure is useful when a port's input buffer is running low on memory resources. In the switch, outbound are packets traversing a single uplink port. When a switch detects that a port's input buffer is nearly full, it simulates a collision so that sending node will defer transmission. The sending node will retry transmissions according to the Ethernet back-off algorithm. Once switch resources are available again, the switch stops sending the collision signal and the nodes can freely transmit packets.

Flow control (full-duplex)

No flow control

Flow control applies only to ports operating in full-duplex mode. It works for full duplex ports the same way as backpressure does for half-duplex ports except that the switch uses a special pause packet instead of a jam signal. The pause packet notifies the other node to stop transmitting for a specified period of time.

Discard broadcast packets

Regular forwarding of broadcasts

Use these two options to have the port either forward broadcast packets or discard them. The default is to forward broadcast packets

Global configuration

This option saves you from having to enter the same configurations on every port. If you select this option, any settings you entered on a port are copied to all the station ports on the switch (but not ports on optional expansion modules).

Port name

The port name field is used to assign a name to the port. Naming ports can make it easier for you to identify the various ports. A name can have up to 20 characters. An example is **Sales - cube 223**.

Refresh

The Refresh button at the bottom of the window queries the switch for the current port settings and displays the settings in the window. This button is available only from a web browser management session

5. Return to the Main Menu.

Configuring Port Trunks

Port trunking is an economical way for you to increase the bandwidth between an AT-8300 Series switch and another network device, such as a server, router, workstation, or another switch. A port trunk is two or more data ports that have been grouped together to increase the bandwidth between a switch and a network node by functioning as one logical path. This increase in bandwidth can prove useful in situations where a single connection between the switch and a node is insufficient to handle the traffic load.

Despite the software configuration and physical connections, there are no data loops in aggregated links because of load balancing. The port trunk always sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

With the AT-8316F Series and AT-8324 switches, you can create port trunks of two, four, or eight ports. You can also trunk the ports on an expansion module to increase the bandwidth from an expansion module to another network device.

Guidelines When creating a port trunk, observe the following guidelines:

Guideline 1: Selecting the Number of Ports in a Trunk

A port trunk must consist of 2, 4, or 8 ports.

Guideline 2: Selecting Ports from the Same Switch in a Stack

The ports of a port trunk must be from the same switch in the stack. A port trunk cannot consist of ports from different switches.

Guideline 3: Using Ports from the Same Group

The ports on the AT-8300 Series switches are divided into groups. The ports for a port trunk must be members of the same group.

The ports on an AT-8324 switch are divided into five groups, as illustrated in Figure 25.

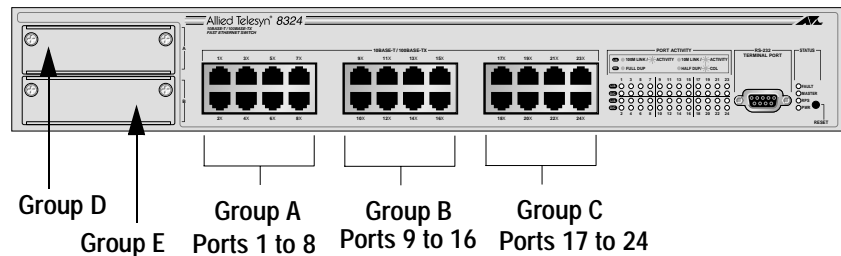


Figure 25 Port Groupings on an AT-8324 Switch

The ports on the AT-8316F/MT and AT-8316F/VF switches are divided into four groups, as shown in Figure 26.

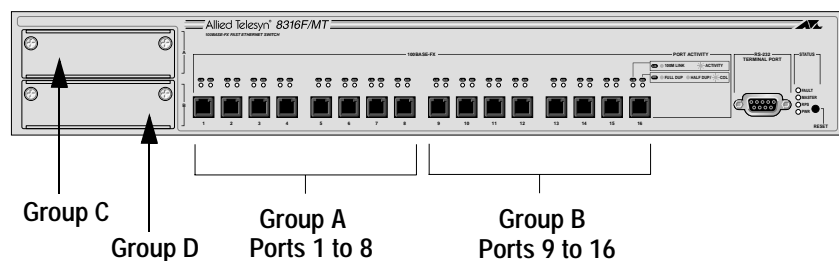


Figure 26 Port Groups on an AT-8316F/MT or AT-8316F/VF Switch

The ports on the AT-8316F/SC switch also are divided into four groups, as shown in Figure 27.

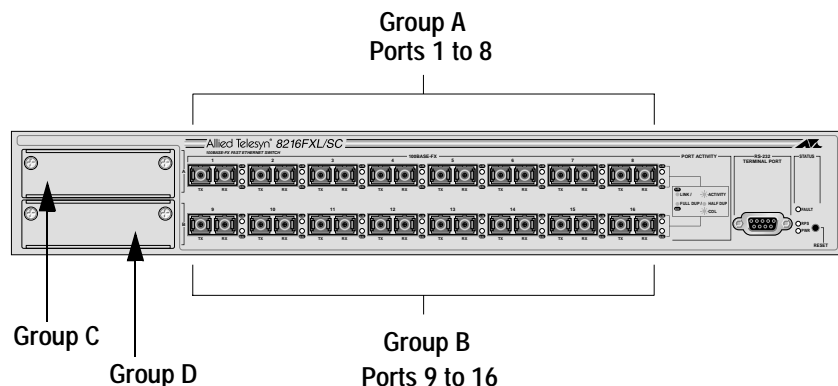


Figure 27 Port Groups on an AT-8316F/SC Switch

The ports of a port trunk must be members of the same group. You cannot use ports from different groups. For example, you could use ports 4 and 5 on an AT-8324 switch as one port trunk, since the ports are members of the same group. However, ports 7, 8, 9, and 10 cannot be combined to form a port trunk on an AT-8324 switch because they belong to different groups.

Guideline 4: Creating Only One Trunk Per Group

Each group of ports on an Ethernet switch can support only one port trunk. For example, the AT-8324 Ethernet switch has three port groups, assuming no expansion modules have been installed in the switch. Consequently, this switch can support three port trunks, one port trunk for each port group. The addition of two expansion modules would enable the switch to support two additional port trunks, one for each module.

Guideline 5: Using Consecutive Ports

The ports of a trunk must be consecutive. For example, you could use ports 4, 5, 6, and 7 as one port trunk, because the ports are consecutive.

Guideline 6: Cabling Based on Port Number

When cabling a trunk, it is important that the order of the connections be identical on both nodes. The lowest numbered port in a trunk must be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port must be connected to the next lowest numbered port on the other device, and so on.

For example, assume that you are connecting a trunk between two AT-8324 switches. On the first AT-8324 switch you had chosen ports 12, 13, 14, 15 from port group two for the trunk. On the second AT-8324 switch you had chosen ports 21, 22, 23, and 24 from port group 3. To maintain the order of the port connections, you connect port 12 on the first AT-8324 switch to port 21 on the second AT-8324, port 13 to port 22, and so on.

Guideline 7: Configuring the Port Parameters of a Port Trunk

The ports in a trunk automatically assume the same configuration (such as VLAN membership) as the configuration of the lowest numbered port. For example, if you create a trunk consisting of ports 4, 5, 6, and 7, port 4 is the master port and its configuration is propagated to ports 5, 6, and 7. As long as the ports are configured as a trunk, you must not change any of the attributes of ports 5, 6, and 7 that might conflict with the settings of port 4.

Guideline 8: Creating Port Trunks on Expansion Modules

The ports on some expansion modules can be grouped together to form port trunks. Refer to Table 4 to determine if your expansion modules support port trunking.

Table 4 Trunked Ports on Expansion Modules

Number of Ports on Expansion Module	Port Trunks
1	Does not support port trunking.
2	One port trunk consisting of two ports.
4	One trunk consisting of two or four ports.

Creating a Port Trunk

To create a port trunk, perform the following procedure:

1. From the Main Menu, select the switch where the port trunk is to be created.
2. From the Main Menu, select *System configuration*.
The System Configuration menu is displayed.
3. Select *Port trunking*.

The Port Trunking window is displayed. The window lists the port groups on the selected switch. The example in Figure 28 shows the five port groups on an AT-8324 switch. Port groups 1, 2, and 3 are for the twisted pair ports, and port groups 4 and 5 are for the optional expansion modules.

Internet Online Help
Internet access required

Online Manual

Technical Support

Send Email

What's New?

Module 1

Ports for port trunk 1 (01 - 08) Enter Reset

Ports for port trunk 2 (09 - 16) Enter Reset

Ports for port trunk 3 (17 - 24) Enter Reset

Ports for port trunk 4 (N/A) Enter Reset

Ports for port trunk 5 (N/A) Enter Reset

Return to Main Menu

Figure 28 Port Trunking Window for an AT-8324 Switch

4. Select the port group in which to create the port trunk and enter the port numbers for the trunk. You can use either of the following formats to enter the port numbers:

Single, consecutive ports (for example, **1,2**)

Range of ports (for example, **10-13**)

Figure 29 is an example. In the example, ports 10 through 13 in port group 2 have been designed as a port trunk.

Internet Online Help
Internet access required

Online Manual

Technical Support

Send Email

What's New?

Return to Main Menu

Module 1

Ports for port trunk 1 (01 - 08) Enter Reset

Ports for port trunk 2 (09 - 16) Enter Reset

Ports for port trunk 3 (17 - 24) Enter Reset

Ports for port trunk 4 (N/A) Enter Reset

Ports for port trunk 5 (N/A) Enter Reset

Figure 29 Example of Two Port Trunks

5. Press <Return> or select Enter.
The port trunk is activated on the switch.
6. If desired, repeat steps 4 and 5 to create another port trunk in another port group on the switch
7. Return to the Main Menu.
8. To confirm the creation of a port trunk, select *Port status and configuration* to display a list of ports. All ports in a port trunk are automatically assigned the name "Trunk" and a number to help you identify the individual port trunks on a switch.
9. Return to the Main Menu.
10. Connect the port trunks on the switch to the end device, being sure to follow the guidelines discussed earlier in this chapter.

Deleting a Port Trunk

To delete a port trunk from a switch, perform the following procedure:

1. From the Main Menu, select the switch with the port trunk to be deleted.

2. From the Main Menu, select *System configuration*.

The System Configuration menu is displayed.

3. Select *Port trunking*.

The Port Trunking window in Figure 28 on page 73 is displayed.

4. *From a web-based Omega session*, delete the ports from the appropriate port group in the window and select Enter.

From a local or Telnet Omega session, enter a space in the port group to be deleted and press Return.

The port trunk is now deleted.

5. Return to the Main Menu.

Configuring a Port Mirror

Port mirroring allows you to monitor the traffic on a port by having both the receive and transmit traffic on a port copied to another port on the switch. This enables you to monitor the traffic on the original port without interrupting network traffic by connecting a network analyzer or RMON port to the port which is functioning as the mirror port.

The port whose traffic is to be monitored is referred to as the source port. The port that will function as the mirror port is referred to as the destination port. When selecting the source and destination ports, be sure to observe the following guidelines.

- ☐ The destination port cannot be used by a network node, such as a workstation or server.
- ☐ Both the source and destination ports must be on the same switch in a stack.
- ☐ You cannot monitor more than one port in a stack at a time.

Enabling Port Mirroring

To enable port mirroring on a switch, perform the following procedure:

1. From the Main Menu, select any switch in the stack. You do not need to select the switch in which you intend to activate port mirroring.
2. From the Main Menu, select *Traffic/Port Mirroring*.

The Port Mirroring window in Figure 30 is displayed.

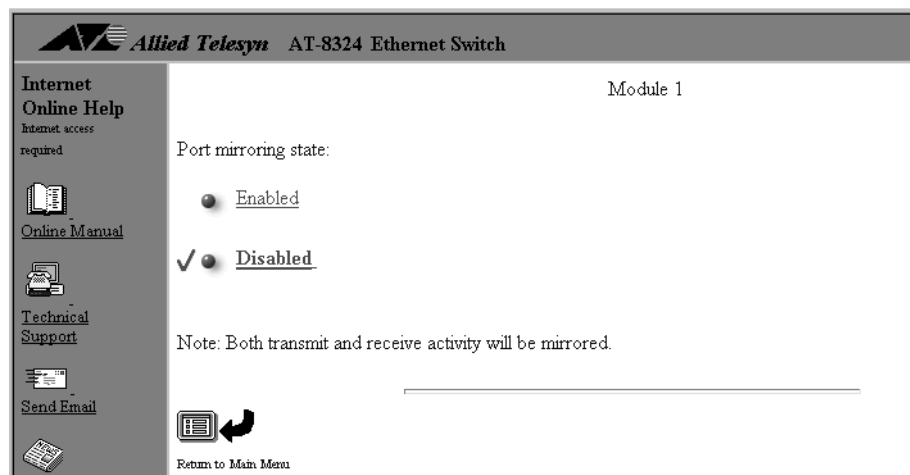


Figure 30 Port Mirroring Window

3. Select *Enabled*.

The prompts in Figure 31 are displayed.

Source Module: Null (not configured)

Source port: Null (not configured)

Destination Module: Null (not configured)

Destination port: Null (not configured)

Figure 31 Source and Destination Port Mirror Prompts

4. Select *Source Module*.

A window is displayed listing the switches in the stack.

5. Select the switch containing the port to be monitored.

6. Select *Source Port*.

A window is displayed listing the ports on the switch.

7. Select the port to be monitored.

8. Select *Destination Module*.

A window is displayed listing the switches in the stack.

9. Select the switch that has the port where the network analyzer will be connected.

10. Select *Destination Port*.

A window is displayed listing the ports on the switch.

11. Select the port where the network analyzer will be connected.

The prompts should now be showing the source and destination switches and ports. Figure 32 is an example.

Source Module: 1

Source port: 9

Destination Module: 1

Destination port: 10

Figure 32 Example of Source and Destination Port Mirror Prompts

The two ports are now configured for port mirroring.

12. Return to the Main Menu.

13. Connect a device, such as a network analyzer, to the destination port or use a remote monitoring program to view the mirrored traffic.

Disabling Port Mirroring

To disable port mirroring on a switch, perform the following procedure:

1. From the Main Menu, select the switch where port monitoring is to be disabled.
2. From the Main Menu, select *Traffic/Port Mirroring*.
The Port Mirroring window in Figure 30 is displayed.
3. Select *Disable*.
The port mirroring feature is now disabled on the switch.
4. Return to the Main Menu.

Configuring Port Security

The Fast Ethernet switch has a port security feature that can be used to enhance network security. This feature allows you to control network access by limiting the number of MAC addresses that are learned on the ports on a switch in a stack.

Note

The port security feature does not apply to ports on any expansion modules installed in the switch.

To set the port security level for the ports on a switch, perform the following procedure:

1. From the Main Menu, select the switch where you want to configure port security.
2. From the Omega Main Menu, select *System Configuration*.

The System Configuration menu in Figure 7 on page 39 is displayed.

3. Select *Security/Source Address Table*.

The following window is displayed:

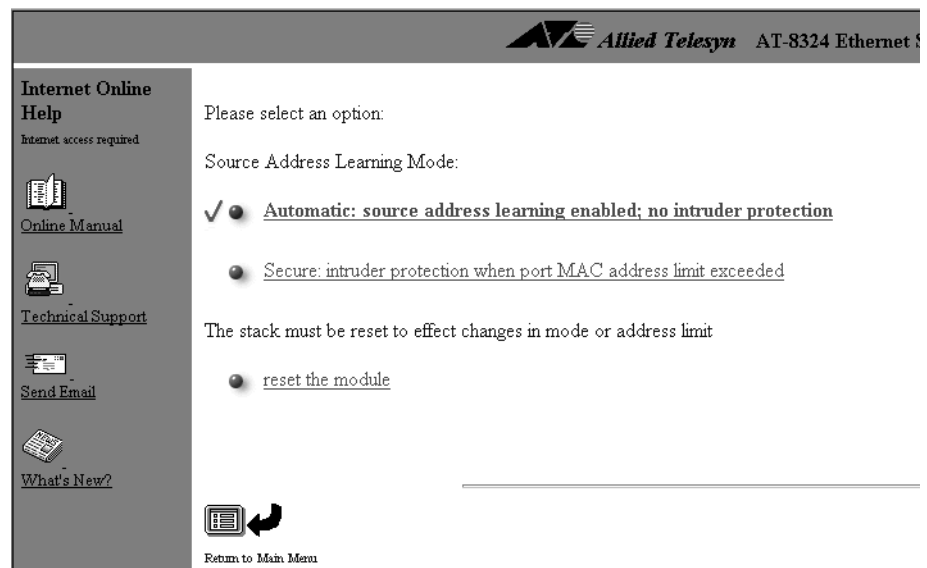


Figure 33 Port Security Window

4. Select the desired port security level. The levels are described here:

Automatic

This selection disables port security. With this option activated, the switch will not restrict the number of MAC addresses that are learned on the switch ports. This is the default setting.

Secure

This selection activates port security. With this option selected, the switch will continue to learn MAC addresses for each port up to a user-configurable maximum number. Once the maximum number has been reached on a port, any frames received on the port from a source with a new MAC addresses will be discarded.

If you select this security feature, all static MAC addresses are deleted and must be reentered. All static MAC addresses are included in the count of maximum addresses that can be learned by a port.

When you select this security level, the following prompts are displayed:

- ☐ Config MAC address limit per port
The stack must be reset to effect changes in mode or address limit
- ☐ reset the module
- Intruder Protection:
 - ☐ Transmit an SNMP Trap if an intruder is detected
 - ✓ ☒ No SNMP Trap if an intruder is detected
 - ☐ Disable the port if an intruder is detected
 - ✓ ☒ Port state unchanged if an intruder is detected

Figure 34 Secure Port Security Prompts

Select the *Config MAC address limit per port* option to display a list of the ports on the switch. In the list, specify the maximum number of MAC addresses that you want each port to be able to learn. The permitted range is 0 to 255. Specifying 0 (zero) means that the port will not stop learning addresses. The default is 0.

The prompts also allow you to control how the switch will respond when a port exceeds the specified number of MAC addresses. You can instruct the switch to send an SNMP trap to the management station or disable the port, or both.

Note

You must reset the stack to activate a change of security level to a switch in the stack. The new security level will not be activated until the stack has been reset.

Chapter 4

Configuring the MAC Address Table

This chapter describes the MAC address table and the static MAC address table. The chapter explains how to view the MAC addresses and how to add and delete entries from the static table. Procedures relating to the MAC address table include the following:

- ☐ **Displaying the MAC Address Table** on page 83
- ☐ **Displaying the MAC Addresses of a Port** on page 84
- ☐ **Displaying the Port Number of a MAC Address** on page 85
- ☐ **Changing the Aging Time of the MAC Address Table** on page 86

Procedures relating to the static MAC address table include the following:

- ☐ **Displaying the Static MAC Address Table** on page 87
- ☐ **Adding Addresses to the Static MAC Address Table** on page 88
- ☐ **Deleting Addresses from the Static MAC Address Table** on page 90
- ☐ **Clearing the Static MAC Address Table** on page 91

This chapter also contains instructions on how to configure multicast addresses for the ports of a switch. The procedures relating to multicast addresses include the following:

- ☐ **Multicast Addresses** on page 92
- ☐ **Changing a Multicast Port Assignment** on page 94
- ☐ **Deleting a Multicast Address** on page 94

MAC Address Table

The MAC address table (also referred to as the forwarding table) is a snapshot of source MAC addresses that a switch has learned and stored in its volatile memory. When a frame is received by a port on a switch, the source address of the frame is inspected to determine whether or not the address is already in the table. If it is not, the switch adds the address to the table.

To prevent the table from becoming filled with addresses of devices that have become inactive and are no longer sending frames, MAC addresses are periodically deleted from the table. An address is deleted if a MAC address in the table does not reappear on any port after a specified period of time has elapsed. The default time period is 300 seconds (5 minutes). This aging time is configurable, as explained in the procedure **Changing the Aging Time of the MAC Address Table** on page 86.

If you reset the switch or remove power, the table is cleared but immediately gets updated as soon as the switch is operational and the ports start to detect MAC addresses in incoming packets.

Each switch in a stack also maintains a static MAC address table. This table contains MAC addresses that are entered manually and are not aged out after a period of time. The only way that a static address is removed is if it is manually deleted from the table. When you enter a static address, you specify the port when the node with the address is connected. Each switch in a stack is responsible for maintaining its own static MAC address table.

Displaying the MAC Address Table

To display the MAC address table for a switch, perform the following procedure:

1. From the Main Menu, select the master or slave switch whose MAC addresses you want to view.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address menu in Figure 35 is displayed.

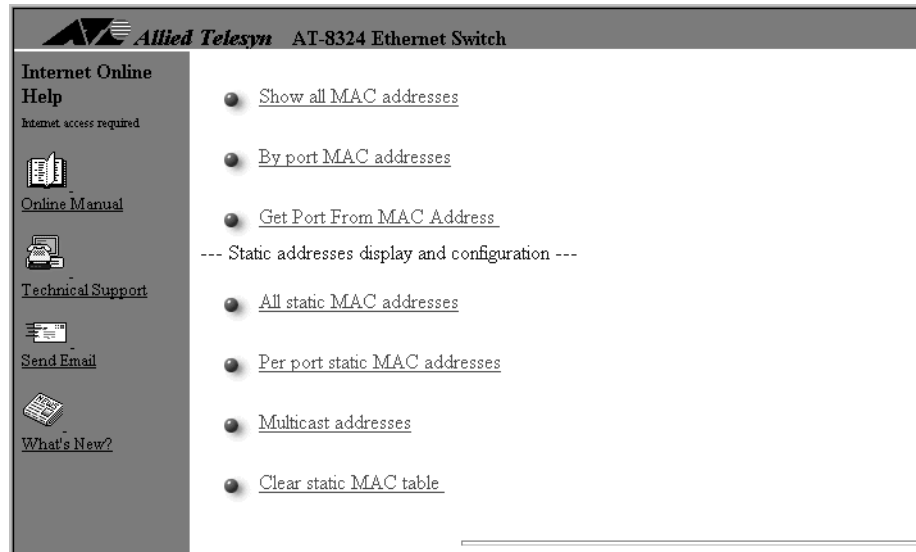


Figure 35 MAC Address Menu

3. Select *Show all MAC addresses*.

The MAC Addresses window is displayed. An example is shown in Figure 36.

MAC Address	Port	VLAN
00000C 938CDC	Port 4 - Accounting1	Default VLAN
0000C0 334CE6	Port 4 - Accounting1	Default VLAN
0000F4 A40D7D	Port 4 - Accounting1	Default VLAN
0000F4 A98B40	Port 4 - Accounting1	Default VLAN
0000F4 C89DCD	Port 4 - Accounting1	Default VLAN
00A0C9 03004F	Port 4 - Accounting1	Default VLAN
00A0C9 0825A5	Port 4 - Accounting1	Default VLAN
00A0CC 3E2463	Port 4 - Accounting1	Default VLAN
00A0D2 18180B	Port 4 - Accounting1	Default VLAN

Figure 36 MAC Address Table

The table lists each MAC address that the stack has learned, the number or name of the port on which the MAC address was detected, and the VLAN to which the port belongs.

Clicking the Refresh button at the bottom of the window queries the switch for the latest MAC addresses and displays an updated version of the MAC address table on the screen.

4. Return to the Main Menu.

Displaying the MAC Addresses of a Port

In addition to displaying all of the MAC addresses stored in a switch, you can also display the MAC addresses associated with a specific port. This allows you to easily determine the MAC addresses of the devices connected to a port on a switch.

To display the MAC addresses for a specific port, perform the following procedure:

1. From the Main Menu, select the switch containing the port whose MAC addresses you want to view.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address menu shown in Figure 35 is displayed.

3. Select *By port MAC addresses*

A list of the ports on the switch is displayed.

4. Select the desired port number from the list.

The MAC Address Table Per Port window is displayed. The window contains the MAC addresses that have been detected on the selected port. Figure 37 is an example of the window.

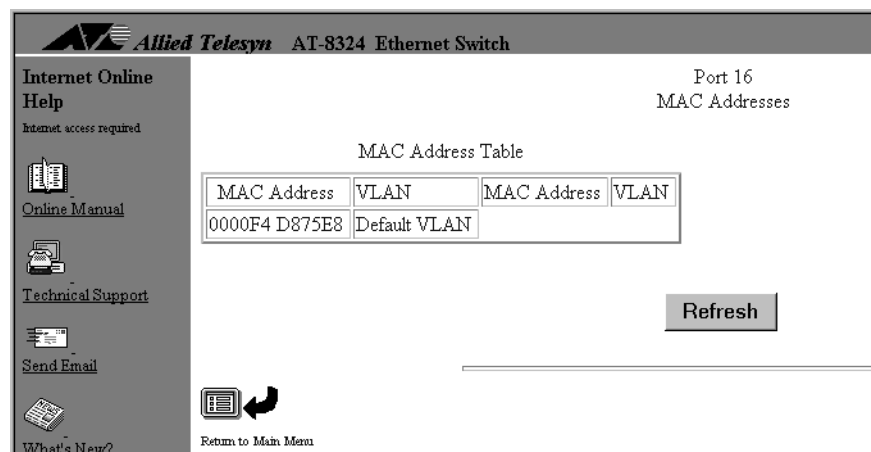


Figure 37 MAC Address Table Per Port Window

5. Return to the Main Menu.

Displaying the Port Number of a MAC Address

The Omega interface allows you to determine the port on which a MAC address is located by specifying the address. This feature is useful in determining the port that a particular device is connected to on a switch.

To display the port number for a specific MAC address, perform the following procedure:

1. From the Main Menu, select the switch where you believe the device is connected.
2. From the Main Menu, select *MAC Address Table*.
3. Select *Get Port From MAC Address*.

The MAC Address prompt shown in Figure 38 is displayed.

Figure 38 MAC Address Prompt

4. Enter the source MAC address. Press <Return> or select Enter.

The MAC address should be entered in the following format:

XXXXXX XXXXXX

The screen displays a window that contains the port on which the MAC address was learned. Figure 39 is an example of the window.

Port	VLAN
16	Default VLAN

Figure 39 MAC Addresses Located on a Port Window

5. Return to the Main Menu.

Changing the Aging Time of the MAC Address Table

If a switch in a stack detects a packet with a new source MAC address, the switch stores the MAC address in its address table. This means the switch has learned about the device that sent packets to the switch. The MAC address table is updated as new MAC addresses are detected. If a MAC address listed in the address table does not appear on any port after a specified period of time, the switch deletes that address from the table. The default aging time is 300 seconds.

To specify a new aging time for the MAC address table, perform the following procedure:

1. From the Main Menu, select the switch in the stack whose MAC aging time you want to change.

Each switch in a stack can have a different MAC aging time.

2. From the Main Menu, select *System Configuration*.

The System Configuration menu in Figure 7 on page 39 is displayed.

3. Select *Default Aging Time*.

The Default Aging Time prompt shown in Figure 40 is displayed.

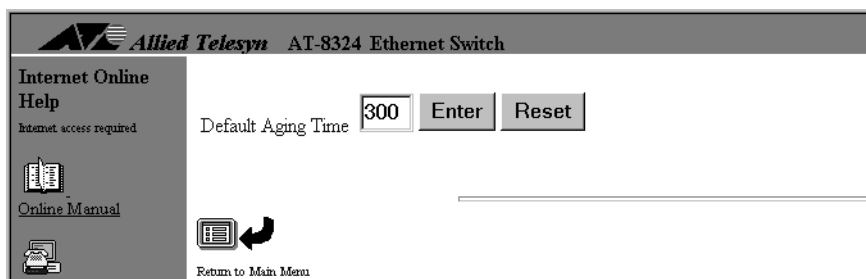


Figure 40 Default Aging Time Prompt

4. Enter a new value (in seconds) in the type-in field. Press <Return> or select Enter. The range is 0 to 999 seconds.

The new value is activated immediately.

Note

Entering a value of 0 (zero) deactivates the MAC aging time parameter. MAC addresses continue to be added to the table until the table is full. Once the table is full, any frame with a new MAC address will be flooded to all appropriate ports.

5. Return to the Main Menu.

Static MAC Address Table

The static MAC table contains a list of the MAC addresses that have been entered manually. You can use the table to specify MAC address for devices connected to ports that might not be learned via the dynamic learning process of the stack. Entering static MAC addresses ensures certain devices access to the switch's ports, because aging time, power failures, or switch resets do not affect the static MAC table. Each switch in a stack maintains its own static address table.

Displaying the Static MAC Address Table

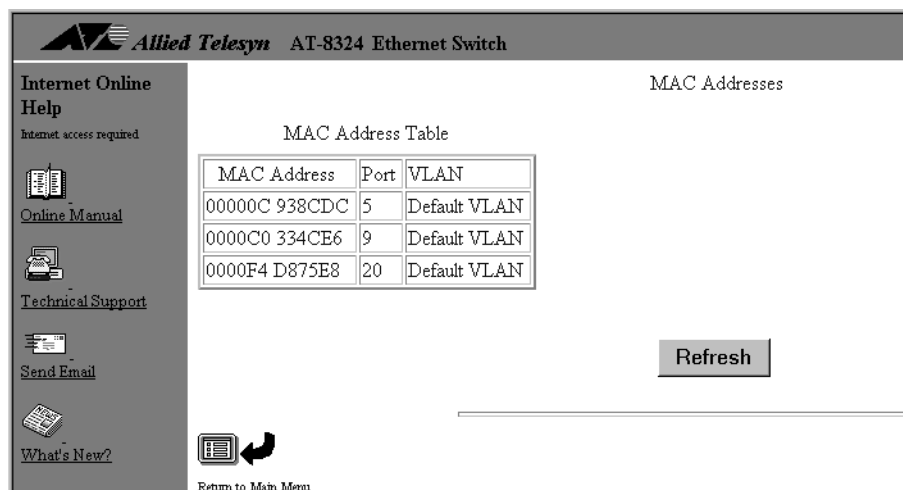
To display the static address table for a switch in a stack, perform the following procedure:

1. From the Main Menu, select the master or slave switch with the static address table you want to view.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address Table menu in Figure 35 is displayed.

3. Select *All static MAC addresses*.

The screen displays previously-added static MAC addresses, their ports, and the VLANs to which the ports belong. The display is for viewing purposes only. Figure 41 is an example of the table.



MAC Address	Port	VLAN
00000C 938CDC	5	Default VLAN
0000C0 334CE6	9	Default VLAN
0000F4 D875E8	20	Default VLAN

Figure 41 Static MAC Address Table Window

4. Return to the Main Menu.

Adding Addresses to the Static MAC Address Table

To add MAC addresses to the static MAC address table, perform the following procedure:

1. Compile a list of the MAC addresses of the devices to be added to the table.
2. From the Main Menu, select the switch in the stack with the port where you want to add static MAC addresses.
3. From the Main Menu, select *MAC Address Table*.

The MAC Address Table menu shown in Figure 35 is displayed.

4. Select *Per port static MAC addresses*.

A list of the ports on the switch is displayed.

5. Select the port where the static MAC address is to be added.

The window in Figure 42 is displayed. The window lists the static addresses already defined for the selected port.

The screenshot shows the web interface of an Allied Telesyn AT-8324 Ethernet Switch. The top header bar displays the Allied Telesyn logo and the device name 'AT-8324 Ethernet Switch'. On the left side, there is a vertical navigation menu with links: 'Internet Online', 'Help', 'Online Manual', 'Technical Support', 'Send Email', and 'What's New?'. The main content area is titled 'Port 4' and 'MAC Addresses'. Below this, there is a section titled 'MAC Address Table' which contains two input fields labeled 'MAC Address' and 'VLAN', followed by another set of 'MAC Address' and 'VLAN' fields. Below these fields are two radio buttons: 'Add MAC address' and 'Delete MAC address'. A 'Refresh' button is located to the right of the radio buttons. At the bottom left of the main area, there is a 'Return to Main Menu' link with a circular arrow icon.

Figure 42 Static MAC Addresses Per Port Window

6. Select *Add MAC Address*.

The window in Figure 43 is displayed. You use this window to specify the MAC address of the device you want to allow access to the port, as well as the name of the VLAN to which the port belongs.

The screenshot shows the web interface of an Allied Telesyn AT-8324 Ethernet Switch. The top header includes the Allied Telesyn logo and the device name. On the left is a navigation menu with links: Internet Online Help, Online Manual, Technical Support, Send Email, and What's New?. The main content area is titled 'MAC Addresses' and 'MAC Address Table'. It contains a table with headers 'MAC Address' and 'VLAN'. Below the table are two input fields: 'VLAN Name' with the text 'Default VLAN' and 'Mac Address' which is empty. Each field has 'Enter' and 'Reset' buttons. At the bottom left is a 'Return to Main Menu' button with a circular arrow icon.

Figure 43 Adding a Static MAC Address

7. In the VLAN Name field, specify the VLAN to which the port belongs. If you have not created any VLANs on the stack, you should enter Default VLAN. Press <Return> or select Enter.
8. In the MAC Address field, enter the static MAC address of the device to have access to the port. Press <Return> or select Enter.

The address should be entered in the following format:

XXXXXX XXXXXX

After adding a static MAC address, return to the Main Menu and select *All static MAC addresses* from the MAC Address Table menu to display the updated table.

The static MAC address appears on the Static MAC table. You can configure only one static MAC address per port.

9. Return to the Main Menu.

Deleting Addresses from the Static MAC Address Table

To delete addresses from the static MAC address table for a port, perform the following procedure:

1. From the Main Menu, select the switch containing the port where the static MAC addresses are to be deleted.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address Table menu in Figure 35 is displayed.

3. Select *Per port static MAC addresses*.

A list of the ports on the switch is displayed.

4. Select the port where the static MAC addresses are to be deleted.

The window in Figure 44 is displayed.

The screenshot shows the web interface of an Allied Telexyn AT-8324 Ethernet Switch. The title bar at the top reads "Allied Telexyn AT-8324 Ethernet Switch". On the left is a sidebar with links: "Internet Online Help" (with a note "Internet access required"), "Online Manual", "Technical Support", "Send Email", and "What's New?". The main content area is titled "MAC Addresses" and "MAC Address Table". It contains a table with two columns: "MAC Address" and "VLAN". The first row shows "00000C 938CDC" under MAC Address and "Default VLAN" under VLAN. Below the table are two input fields: "VLAN Name:" with a text box containing "Default VLAN" and buttons "Enter" and "Reset"; and "Mac Address:" with an empty text box and buttons "Enter" and "Reset". At the bottom left is a "Return to Main Menu" link with a back arrow icon.

MAC Address	VLAN
00000C 938CDC	Default VLAN

VLAN Name:

Mac Address:

[Return to Main Menu](#)

Figure 44 Deleting a Static MAC Address Window

5. In the VLAN Name field, enter the name of the VLAN to which the port belongs. Press <Return> or select Enter.
6. In the MAC Address field, enter the MAC address to be deleted from the static table. Press <Return> or select Enter.

The address is now deleted from the static MAC address table.

After deleting a static MAC address, return to the Main Menu and select *All static MAC addresses* from the MAC Address Table menu to display the updated table.

7. Return to the Main Menu.

Clearing the Static MAC Address Table

To clear all addresses from the static MAC address for a switch in a stack, perform the following procedure:

1. From the Main Menu, select the switch containing the static address table to be cleared.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address Table menu shown in Figure 35 is displayed.

3. Select *Clear static MAC table*.
4. Select Yes to confirm or No to cancel the procedure.

If you select Yes, all of the static address entries are deleted from the switch.

5. Return to the Main Menu.

Multicast Addresses

A multicast is a special form of broadcast where copies of a packet are delivered to a specific group of end stations. This differs from a broadcast, which is a transmission that sends copies of a packet to all end stations on the network.

A multicast address is a destination address. You can configure 10 (ten) multicast addresses per switch in a stack. Configuring a multicast address enables you to restrict certain packets to only go to a group of ports. For example, you can have a server running some special applications and you do not want all end stations in the network to receive packets from this server.

Configuring a Multicast Address

To enter a multicast address into the MAC address table of a switch in a stack, perform the following procedure:

1. From the Main Menu, select the switch in the stack that has ports to receive the multicast transmission.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address Table menu is displayed.

3. Select *Multicast addresses*.

The Multicast Address Menu shown in Figure 45 is displayed.

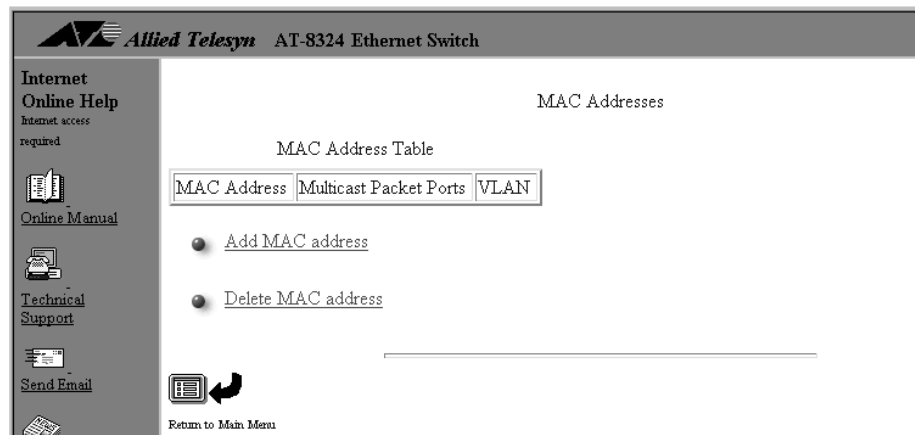


Figure 45 Multicast Address Menu

4. Select *Add MAC address*.

The Adding a Multicast Address window shown in Figure 46 is displayed.

Figure 46 Adding a Multicast Address Window

5. In the VLAN Name field, enter the name of the VLAN to receive the multicast frames. Press <Return>.
6. In the MAC Address field, enter the MAC address of the multicast stream. Press <Return>.
7. In the Ports for Multicast field, enter one or more port numbers that are members of the specified VLAN and that are to receive the multicast packets from the device. Press <Return>.

You can use one of the following formats to specify the port numbers:

Single port (for example, 1)

Several ports separated by comma (for example, 3, 8, 22)

Range of ports (for example, 4-16)

All ports by entering the word "all"

You can combine these different formats in a single line.

Any port can have more than one multicast address associated with it. The number of multicast addresses you can configure is limited to ten (10) per switch.

Omega confirms a successful operation with the message *MAC address added* and the MAC address.

8. Return to the Main Menu.

Changing a Multicast Port Assignment

To add or remove ports from a multicast MAC address assignment, re-enter the multicast MAC address and the new port assignments by performing the instruction in the previous section. This will overwrite the old port assignments with the new port information.

Deleting a Multicast Address

To delete a multicast address from the MAC address table, perform the following procedure:

1. From the Main Menu, select the switch with the multicast address to be deleted.
2. From the Main Menu, select *MAC Address Table*.

The MAC Address Table menu is displayed.

3. Select *Multicast addresses*.

The menu in Figure 45 on page 4-92 is displayed.

4. Select *Delete MAC Address*.

The Deleting a Multicast Address window in Figure 47 is displayed.

Internet Online
Help
Internet access required

Online Manual

Technical Support

Send Email

What's New?

Return to Main Menu

MAC Addresses

MAC Address Table

MAC Address	Multicast Packet Ports	VLAN
00000C 938CDC	13	Default VLAN

VLAN Name:

Mac Address:

Figure 47 Deleting a Multicast Address Window

5. In the VLAN Name field, enter the name of the VLAN from which the multicast address is to be deleted.
6. In the MAC Address field, enter the MAC address to be deleted. Press <Return> or select Enter.

The multicast address is now deleted.

7. Return to the Main Menu.

Chapter 5

Configuring Virtual LANs and Quality of Service

This chapter contains the procedures for creating and modifying VLANs. It also explains the Quality of Service (QoS) feature. This chapter contains the following sections:

- ❑ **Creating a New VLAN** on page 98
- ❑ **Modifying a VLAN** on page 105
- ❑ **Deleting a VLAN** on page 106
- ❑ **Activating or Deactivating the Basic VLAN Mode** on page 107
- ❑ **Assigning the CPU Management Port to a VLAN** on page 110
- ❑ **Configuring Quality of Service** on page 108

Note

For background information on VLANs, refer to **Appendix A, Introduction to Virtual LANs** on page 139.

The default VLAN configuration for an AT-8300 stack is one VLAN. This VLAN is named Default VLAN. The Default VLAN has a VLAN ID of 1. All the ports of all the switches in the stack are port-based (untagged) members of the Default VLAN and are assigned a PVID of 1. Thus, all ports in the stack are on a common broadcast domain. A stack can support up to 254 VLANs. In most situations, you will probably find this single broadcast domain settings acceptable and will not need to modify the switch's VLAN settings.

Note

You should use caution when using the Spanning Tree Protocol (STP) and VLANs. The switch has only one spanning tree domain.

Creating a New VLAN

This section contains the procedure for creating a new VLAN in a stack. The procedure explains how to assign a name to the VLAN and how to specify which ports will be members of the new VLAN.

Note

For background information on VLANs, refer to **Appendix A, Introduction to Virtual LANs** on page 139.

To create a new VLAN, perform the following procedure:

1. From the Main Menu, select a switch in the stack with ports that will be members of the new VLAN. If the new VLAN will contain ports from several switches in the stack, select any one of the switches.
2. From the Main Menu, select *Virtual LANs/QoS*.

Note

If the Omega Main Menu does not include the *Virtual LANs/QoS* selection, the stack is operating in the Basic VLAN Mode. To create VLANs, you must deactivate the Basic VLAN Mode, as explained in **Activating or Deactivating the Basic VLAN Mode** on page 107.

The Virtual LAN/QoS menu in Figure 48 is displayed.

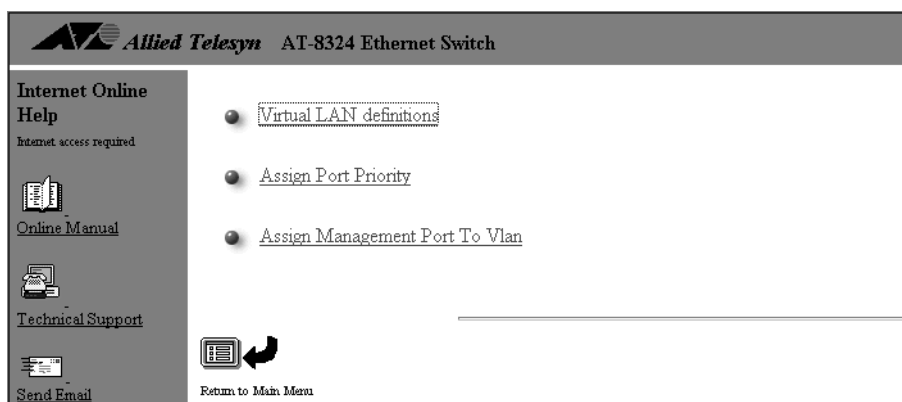


Figure 48 Virtual LAN/QoS Menu

3. Select *Virtual LAN definitions*.

The program displays the VLANs window. This window lists the VLANs currently existing on the stack. The window provides the name of each VLAN along with the ports on the currently selected switch that are members of the VLAN. Figure 49 is an example of the window.

Page 1

VLAN Name	ID	Untagged VLAN Ports	Tagged Ports On Vlan
Default VLAN	1	6-7, 12-24	
Sales	2	2-5	9
Production	3	8, 10-11	9
Engineering	4		
Technical Support	5		

[Add new table entry](#)

[Refresh](#)

[Return to Main Menu](#)

Figure 49 VLANs Window

The example shows that there are five VLANs on the stack: Default VLAN, Sales, Production, Engineering, and Technical Support. The numbers following each VLAN indicate the VID number of the VLAN and the untagged and tagged ports that belong to the VLAN. For example, the Production VLAN has the VID number of 3. Ports 8, 10, and 11 on the currently selected switch have been assigned to this VLAN as untagged ports and port 9 on the switch has been designated as a tagged port.

The example VLANs window also includes the two VLANs Engineering and Technical Support. The currently selected switch does not have ports that are members of these VLANs, which is why there are no ports listed after the VLAN names.

4. Select *Add new table entry*.

The VLAN Configuration window shown in Figure 50 is displayed. You use this window to specify the parameters for the new VLAN, such as its name and the ports on the currently selected switch that will be members of the VLAN.

Internet Online Help
Internet access required

Online Manual

Technical Support

Send Email

What's New?

200.24

VLAN Name: Enter Reset

(or enter a single '*' to delete this entry)

ID Enter Reset

All Ports Enter Reset

On Vlan

(Example: 1,3,8-14 or all)

Tagged Ports Enter Reset

On Vlan

Untagged VLAN Ports

☒ UPDATE this VLAN or NO UPDATE and

Figure 50 VLAN Configuration Window

5. Select the VLAN Name field and enter a name for the new VLAN (for example, Marketing). Press <Return>.

After entering the name for the new VLAN, the VLAN ID number automatically increments to the next available number. For example, if this is the first VLAN that you are adding to the stack, the VID number increments to 2.

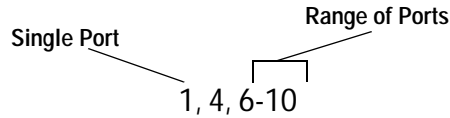
6. If desired, select the ID field and change the VLAN ID number. Press <Return>. For the range of this parameter, refer to **VLAN Identifier** on page 141

Note

Allied Telesyn highly recommends that you use the VLAN ID (default) supplied by the system. Although you can change VLAN IDs to suit your specific needs, changing them requires a more advanced understanding of VLAN tagging.

7. Select the In the All Ports on VLAN field and specify the ports (both tagged and untagged) on the currently selected switch that are to be members of this new VLAN. Press <Return>.

As shown below, you can specify the ports individually or in a range or both. By entering the word "All" in this field, all ports on the switch will be included in the new VLAN.



Ports on expansion modules, if installed, are included by default in the Ports on VLAN field. If desired, these ports can be removed from the field so that they will not be a part of the VLAN.

8. If the VLAN will contain tagged ports on the selected switch, select the Tagged Ports on VLAN field and specify which ports, if any, will be tagged ports. Press <Return>.
9. Select *Update this VLAN*.

The new VLAN is now created on the stack.

10. Return to the Main Menu.
11. To add ports to this VLAN from other switches in the stack, perform the procedure, **Modifying a VLAN** on page 105.

Example of Creating a Port-based VLAN

This procedure creates the Sales VLAN illustrated in Figure 61 on page 144. This VLAN is port-based because all of the ports are untagged ports. To create the Sales VLAN, you would perform the following steps:

1. From the Main Menu, select the master switch (stack ID 1).
2. From the Main Menu, select *Virtual LAN/QoS*.
3. From the Virtual LAN/QoS menu, select *Virtual LAN Definition*.
4. From the Virtual LAN definition window, select *Add New Entry*.
5. In the VLAN Name field, enter the name Sales. Press <Return>.
6. Either enter a new value for the ID of the VLAN by entering a new number in the ID field and pressing <Return>, or accept the default value of 2.
7. In the All Ports on VLAN field, enter the following and press <Return>:

1-7

These are the untagged ports on the master switch that are to be a part of the Sales VLAN.

Note

Since this VLAN will not contain any tagged ports, the Tagged Ports in VLAN field is left empty.

8. Select *Update this VLAN*.

The VLAN titled Sales has now been created in the stack. The new VLAN consists of ports 1 through 7 on the master switch.

9. Return to the Main Menu.
10. From the Main Menu, select the slave switch (stack ID 2).
11. From the Main Menu, select *Virtual LAN/QoS*.
12. From the Virtual LAN/QoS window, select the Sales VLAN.

The VLAN Configuration window for the Sales VLAN is displayed.

13. In the All Ports on VLAN field, enter the following. Press <Return>.

1-4, 8

Ports 1 to 4 and port 8 on the slave switch will be untagged ports of the Sales VLAN.

Since there will not be any tagged ports in this VLAN, the Tagged Ports in VLAN field is left empty.

14. Select *Update this VLAN*.
15. Return to the Main Menu.

The Sales VLAN now exists in the AT-8300 stack. It contains ports from both the master switch and the slave switch.

Example of Creating a Tagged VLAN

This procedure creates the Production VLAN on the AT-8300 stack illustrated in Figure 62 on page 150. This VLAN contains several tagged ports in addition to untagged ports. To create the Production VLAN, you would perform the following steps:

1. From the Main Menu, select the master switch (stack ID 1).
2. From the Main Menu, select *Virtual LAN/QoS*.
3. From the Virtual LAN/QoS menu, select *Virtual LAN Definition*.
4. From the Virtual LAN definition window, select *Add New Entry*.
5. In the VLAN Name field, enter the name Production. Press <Return>.
6. Either enter a new value for the ID of the VLAN by entering a new number in the ID field or accept the default value by pressing <Return>.
7. In the All Ports on VLAN field, enter the following and press <Return>:

11, 19-24

These are the ports, both tagged and untagged, on the master switch that are to be a part of the Production VLAN. It is important to note that in this field you specify both types. The All Ports on VLAN field must contain tagged ports, if there will be any, in addition to the untagged ports.

8. In the Tagged Ports in VLAN field, enter the following and press <Return>:

11

Port 11 on the master switch in the Production example will function as a tagged port. The port will provide a common uplink to the router and WAN for both the Sales and Production VLANs. This field would be left empty if there were to be no ports functioning as tagged ports on the selected switch.

9. Select *Update this VLAN*.

The VLAN titled Production has now been created in the stack. The new VLAN consists of ports 11 and 19 to 24 from the master switch.

10. Return to the Main Menu.
11. From the Main Menu, select the slave switch (stack ID 2).
12. From the Main Menu, select *Virtual LAN/QoS*.
13. From the Virtual LAN/QoS window, select the Production VLAN.

The VLAN Configuration window for the Production VLAN is displayed.

14. In the All Ports on VLAN field, enter the following and press <Return>:

10, 16, 22-24

These are the ports, both tagged and untagged, on the slave switch that are to be a part of the Production VLAN. Ports 22 through 24 will be untagged ports while ports 10 and 16 will be tagged.

15. In the Tagged Ports on VLAN field, enter the following and press <Return>:

10, 16

These are the two ports on the slave switch that are to be tagged ports in the Production VLAN. Port 10 functions as an uplink to the AT-8224XL switch. Port 16 is connected to a IEEE 802.3Q-compliant server, meaning that it can be shared by the two VLANs.

16. Select *Update this VLAN*.

17. Return to the Main Menu.

The Production VLAN now contains ports from both the master switch and the slave switch. Additionally, port 11 on the master switch and ports 16 and 18 on the slave switch have been designated as tagged ports, meaning they can be members of more than one VLAN.

Modifying a VLAN

This procedure explains how to add or delete ports from an existing VLAN. You can also change a port from untagged to tagged, or vice versa. To modify a VLAN, perform the following procedure:

1. From the Main Menu, select the switch in the stack that contains a port to be added or removed from the VLAN.
2. From the Main Menu, select *Virtual LANs/QoS*.

The Virtual LAN/QoS menu shown in Figure 48 is displayed.

Note

If the Omega Main Menu does not include the *Virtual LANs/QoS* selection, the stack is operating in the Basic VLAN Mode. To modify a VLAN, you must deactivate the Basic VLAN Mode, as explained in **Activating or Deactivating the Basic VLAN Mode** on page 107.

3. Select *Virtual LAN definitions*.

The VLAN window shown in Figure 49 is displayed. The window lists the current VLANs in the stack, along with the untagged and tagged ports on the currently selected switch that have been assigned to the VLANs.

4. Select the name of the VLAN to be modified.

The VLAN Configuration window for the selected VLAN is displayed. An example is shown in Figure 50 on page 100.

5. Select the All Ports on VLAN field and revise the port list for the VLAN. Press <Return>.

If you are adding ports from the currently selected switch to the VLAN, be sure to include both tagged and untagged ports.

6. Select the Tagged Ports on VLAN field and enter the revised tagged port list for the VLAN. Press <Return>.
7. Select *Update this VLAN*.

The changes to the port assignments to the VLAN are activated immediately. Ports removed from the VLAN are returned to the Default VLAN. The software also checks if an untagged port already belongs to another VLAN. If it does, a message indicates that the port will be removed from the old VLAN. The PVIDs are also adjusted for the ports on both old and new VLANs.

8. Return to the Main Menu.

Deleting a VLAN

To delete a VLAN from a stack, perform the following procedure:

1. From the Main Menu, select any switch in the stack.

It does not matter which switch in a stack you select when deleting a VLAN.

2. From the Main Menu, select *Virtual LANs/QoS*.

The Virtual LAN/QoS menu in Figure 48 on page 98 is displayed.

3. Select *Virtual LAN definitions*.

The VLANs window in Figure 49 on page 99 is displayed.

4. Select the name of the VLAN to be deleted.

Note

You cannot delete the Default VLAN.

The current configuration for the selected VLAN is displayed. An example is shown in Figure 50 on page 100.

5. Select the VLAN Name field and enter an asterisk (*) in the field. Press <Return>.
6. Select *Update this Vlan*.

The VLAN is now deleted from the stack. All ports in the VLAN are returned to the Default VLAN.

7. Return to the Main Menu.

Activating or Deactivating the Basic VLAN Mode

This section contains the procedure for activating or deactivating the Basic VLAN Mode.

Note

For information on the Basic VLAN Mode, refer to **Basic VLAN Mode** on page 152 in **Appendix A, Introduction to Virtual LANs**.

To activate or deactivate the Basic VLAN Mode, perform the following procedure:

1. From the Main Menu, select any switch in the stack.
2. From the Main Menu, select *System Configuration*.

The System Configuration menu is displayed, as shown in Figure 7 on page 39.

3. Select *Switch-mode Selection*.
4. The Switch Mode window shown in Figure 51 is displayed.

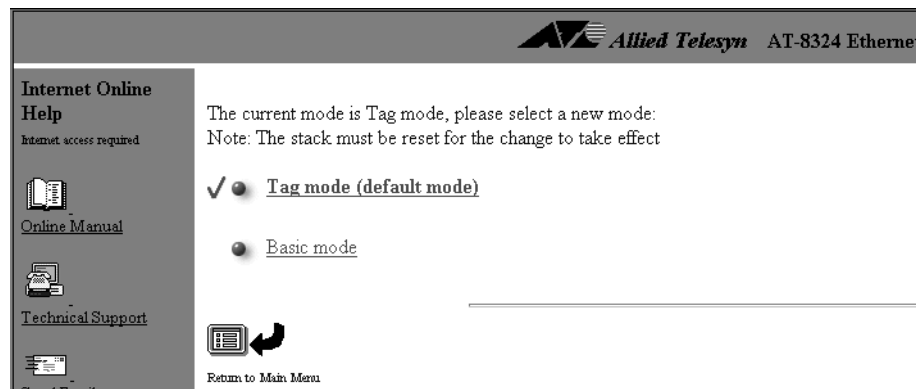


Figure 51 Switch Mode Window

5. To activate the Basic Switch Mode, select *Basic Mode* from the window. To deactivate Basic Switch Mode and so be able to create and modify port-based and tagged VLANs, select *Tag Mode (default mode)* from the window.
6. Return to the Main Menu.
7. It is recommended that you reset the stack after either activating or deactivating the Basic VLAN Mode. For instructions, refer to **Resetting a Stack** on page 51 in Chapter 2.

Configuring Quality of Service

The AT-8324 and AT-8316F Series Switches support Quality of Service (QoS) as defined in the IEEE 802.1p standard. QoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, that can be adversely affected by packet transfer delays.

Prior to QoS, network traffic was handled in a best-effort manner, where packet forwarding was typically performed on a first-in, first-out basis. File transfer delays did occur, but were mostly transparent to network users. But with the introduction of time-critical applications, packet transfer delays can be problematic. For example, transfer delays of voice transmission can result in poor audio quality.

QoS was designed to address this problem. The IEEE 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest priority.

The AT-8324 and AT-8316F Series Switches feature two priority egress queues: high and normal. Packets with priority values 0 through 3 are placed in the normal priority egress queue. Packets with priority values 4 through 7 are placed in the high priority egress queue.

When a tagged packet enters a switch port, the switch responds to the priority in the tag and forwards the packet accordingly. If desired, you can configure the individual ports on the switch so that the priority level in a tagged frame is ignored and that the tagged packets received on a port are automatically assigned to either the normal or high priority queue, regardless of the priority level in the packet. Consequently, the switch will forward a tagged frame according to the port priority level and not to the priority level in the tagged frames. However, the switch does not alter the priority level in the packet, so that when the switch transmits the packet, its original packet priority level is unaltered.

Note

The priority value in the packet is forwarded unchanged except in the rare case when VLAN ID equals 0 (a special priority-tagged frame with no VLAN ID information). In this case, packets with priority values 0 through 3 will be mapped to priority 0, and packets with priority values 4 through 7 will be mapped to priority 7.

The options available are:

- ☐ Keep or override the default tag value.
- ☐ Set the priority to high or normal.

To adjust the settings for priority queueing, perform the following procedure:

1. From the Main Menu, select the switch containing the port whose priority settings are to be changed.
2. From the Main Menu, select *Virtual LANs/QoS*.

Note

If the Omega Main Menu does not include the *Virtual LANs/QoS* selection, the stack is operating in the Basic VLAN Mode. Altering the priority queue settings is not allowed when a stack is operating in the Basic VLAN Mode.

3. From the Virtual LANs/QoS menu, select *Assign Port Priority*. The Omega program displays a list of the ports on the selected switch.
4. Select a port number to display the following screen (Port 4 is used as an example):

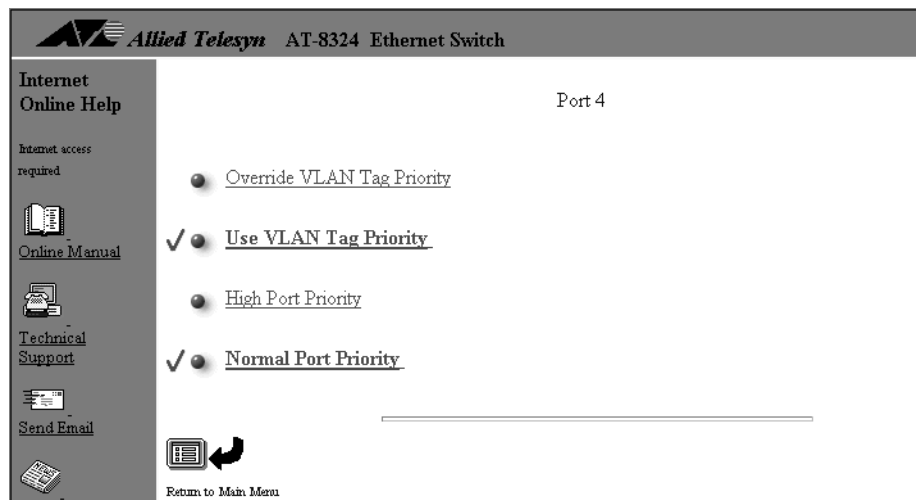


Figure 52 Port Priority Setting Window

5. Adjust the settings as desired.

To override the priority levels specified in the tagged frames received on the port, select *Override VLAN Tag Priority*. Then select either *High Port Priority* to have the tagged frames entering the port handled by the high priority queue or *Normal Port Priority* to have the frames handled by the normal queue.

Selecting the *Use VLAN Tag Priority* option instructs the switch to use the priority level contained in the tagged frames, and disables any port priority setting. This is the default setting.

6. Return to the Main Menu.

Assigning the CPU Management Port to a VLAN

This section contains the procedure for assigning the CPU management port of the master switch to a VLAN. By default, the management port is assigned to the VLAN named Default VLAN.

Note

This procedure should be performed with caution. The CPU management port must be assigned to the same VLAN that contains the ports to which your remote management stations are connected. Assigning the management port to a VLAN that does not contain the ports for your remote management stations will prevent you from being able to manage the stack remotely.

To assign the CPU port to a VLAN, perform the following procedure:

1. From the Main Menu, select the master switch.

Note

You must select the master switch to perform this procedure. Do not select a slave switch.

2. From the Main Menu, select *Virtual LANs/QoS*.

The Virtual LAN/QoS menu in Figure 48 on page 98 is displayed.

3. Select *Assign Management Port to VLAN*.

The window in Figure 53 is displayed.

The screenshot shows the web interface of an Allied Telesyn AT-8324 Ethernet Switch. The title bar at the top reads "Allied Telesyn AT-8324 Ethernet Switch". On the left is a navigation menu with links: "Internet", "Online Help", "Internet access required", "Online Manual", "Technical Support", and "Send Email". The main content area displays a "NOTE : Input Port Used must be on same VLAN as the Managment Port or Management Connection will be lost!!". Below the note, there is a label "Management Port Vlan" followed by a text input field containing the number "1", and two buttons labeled "Enter" and "Reset". At the bottom, there is a "Return to Main Menu" link with a circular arrow icon.

Figure 53 VLAN Assignment for CPU Management Port

4. In the Management Port VLAN field, specify the VID of the VLAN to which the management port is to be assigned. Press <Return>.

Note

The VLAN must already exist. You cannot assign the management port to a VLAN that does not exist. The value 1 is the VID for the Default VLAN.

5. Return to the Main Menu.

Chapter 6

Displaying Ethernet Statistics

The Omega interface allows you to view a wide range of statistics that you can use in diagnosing a problem and isolating it to a specific port. Menu selections enable you to view both received or transmitted frame statistics at either the switch or the port level. You can also view RMON statistics at either the switch or port level.

This chapter contains the following procedures:

- ❑ **Displaying Statistics for Received Frames** on page 114
- ❑ **Displaying Statistics for Transmitted Frames** on page 118
- ❑ **Displaying RMON Statistics for a Switch** on page 120
- ❑ **Displaying RMON Statistics for a Port** on page 121
- ❑ **Resetting the Statistics Counters** on page 122
- ❑ **Interpreting the Graphs** on page 123

Displaying Statistics for Received Frames

To display statistics for received frames at either the switch or the port level, perform the following procedure:

1. From the Main Menu, select the switch whose statistics you want to view.
2. From the Main Menu, select *Ethernet Statistics*.

The Receive Statistics Graph window for the switch is displayed. Figure 54 is an example of the window.

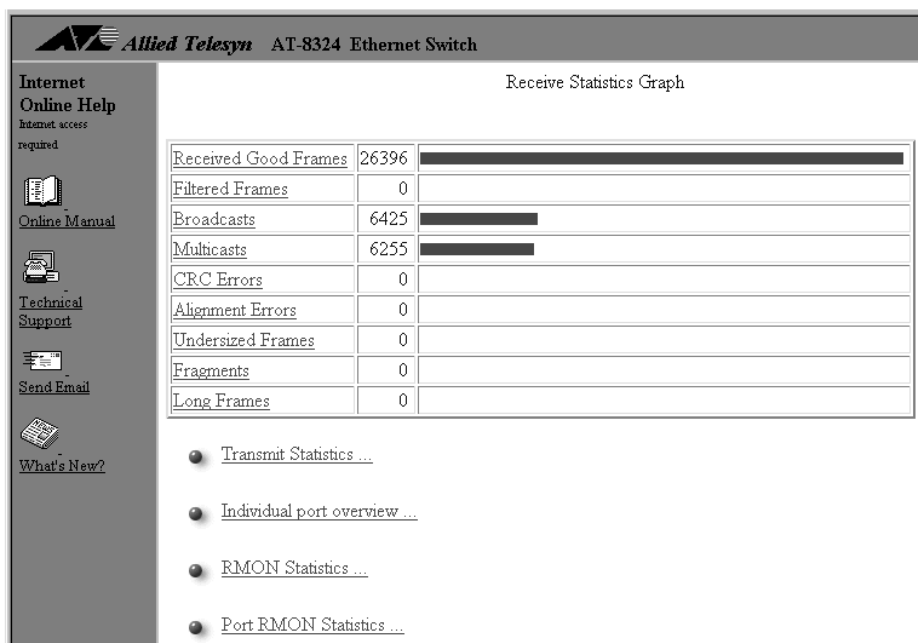


Figure 54 Graph of Received Frames, Switch Level

The graph shows the types of frames the switch has received over a period since the switch's last reset or since someone has last set the counters to 0 (zero).

Table 5 defines the different types of received frames.

Table 5 Received Ethernet Frames

Frame Type	Description
Received Good Frames	Total number of frames received by the switch since the last reset.
Filtered Frames	Frames received by the switch but not forwarded because the destination is within the same LAN segment, therefore, the frame was already seen by all nodes on the segment.
Broadcasts	Frames received by the switch destined for ALL nodes on the network, excluding multicast frames.
Multicasts	Frames received by the switch destined for multiple but specific addresses, excluding broadcast frames.
CRC Errors	Frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes).
Alignment Errors	Frames with a non-integral number of bytes, that is, frame length in bits are not evenly divisible by 8, but with the proper length (64-1518 bytes).
Undersized Frames	Frames less than the minimum specified by IEEE 802.3 (64 bytes including the CRC); also called runts.
Fragments	Total undersized frames, frames with alignment errors, and frames with FCS errors (CRC errors).
Long Frames	Frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC).

3. To view received frame statistics for a particular port, do either of the following:
 - a. Select *Individual port overview* and then a port. The frames statistics for the selected port are displayed. Figure 55 is an example of the window.

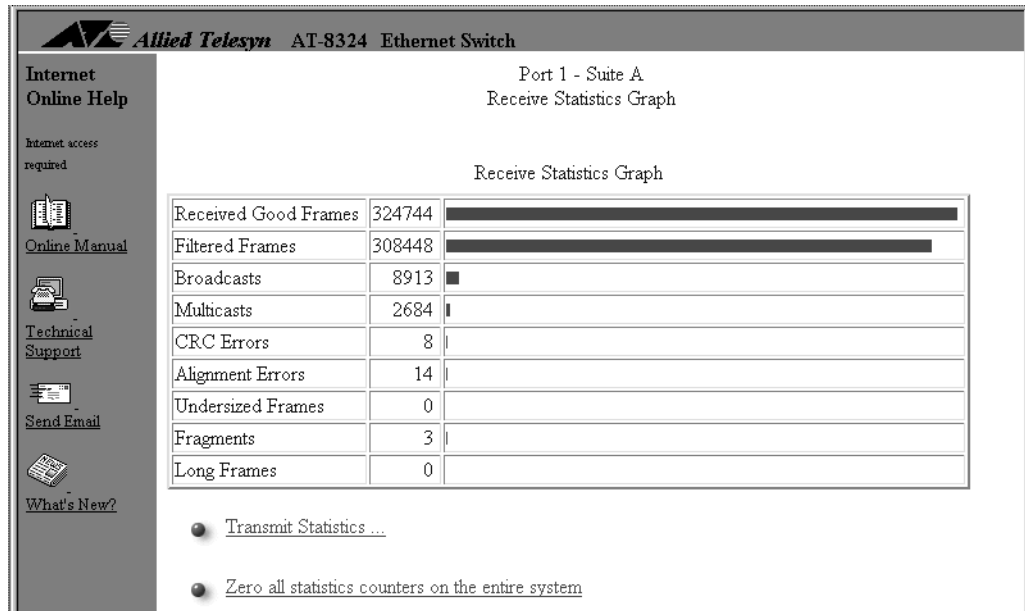


Figure 55 Graph of a Port's Received Frames

- b. Select a frame type from the Receive Frames window. The statistics for the selected frame type for all of the ports is displayed. A example is shown in Figure 56.

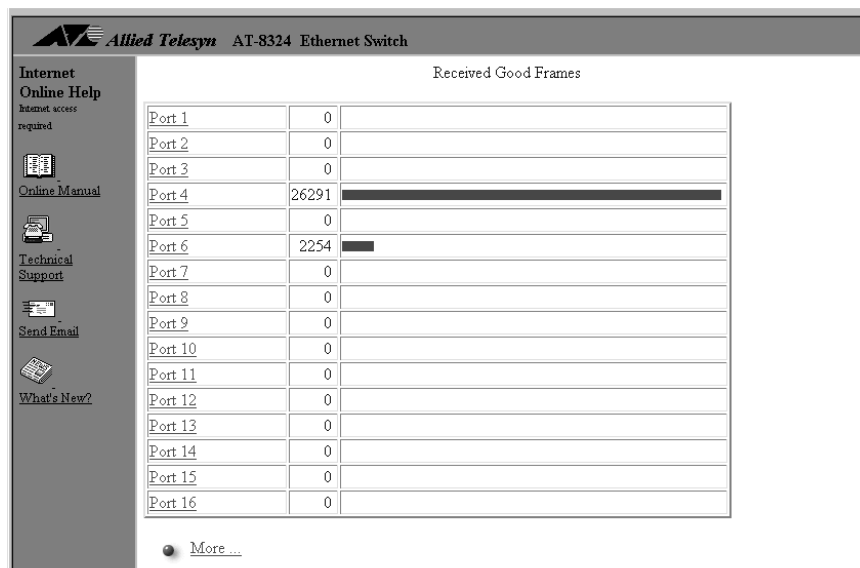


Figure 56 Sample Graph of a Single Frame Type on All Ports

You can also view an individual port's receive statistics by selecting the *Port status and configuration* option from the Main Menu, and choosing a port number.

4. To clear the graph, select *Zero all statistics counters on the entire system*.
5. Return to the Main Menu.

Displaying Statistics for Transmitted Frames

To display statistics for transmitted frames at both the switch and port level, perform the following procedure:

1. From the Main Menu, select the switch whose statistics you want to view.
2. From the Main Menu, select *Ethernet Statistics*.

The Receive Statistics Graph in Figure 54 is displayed.

3. Select *Transmit Statistics*.

The window in Figure 57 is displayed. The window displays the transmit frame statistics for the entire switch. The graph shows the types of frames the switch has transmitted over a period since the switch's last reset or since someone has set the counters to 0 (zero).

Transmit errors should be very small. The switch may receive a number of bad frames, but the switch drops those and sends only good frames.

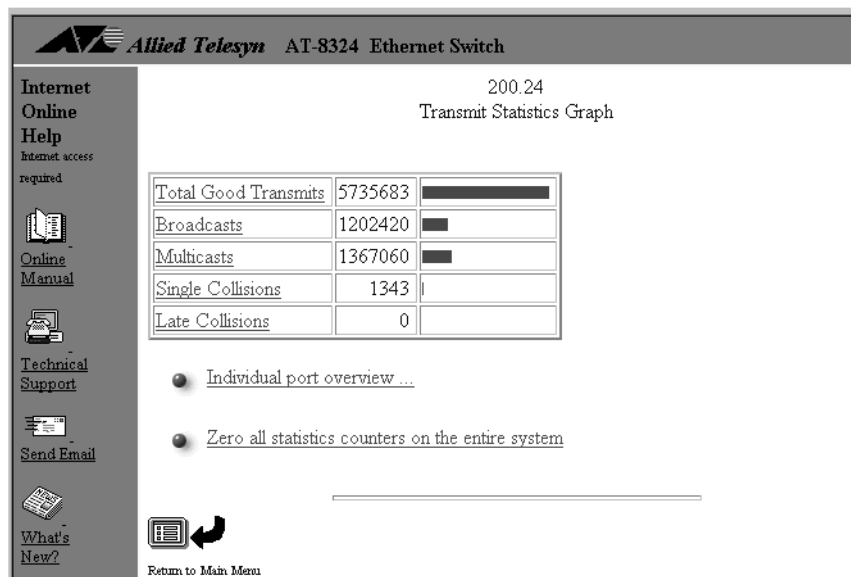


Figure 57 Sample Graph of Transmitted Frames Window

Table 6 defines the statistics.

Table 6 Transmit Frames

Frame Type	Description
Total good transmits	Total frames transmitted by the switch without errors since the last reset.
Broadcasts	Frames forwarded by the switch destined for ALL nodes on the network, excluding multicast frames.
Multicasts	Frames forwarded by the switch destined for multiple but specific addresses, excluding broadcast frames.
Single collision	Frames from two ports that collided because they were sent at the same time; considered normal.
Late collisions	Collisions that occur after 64-byte times of the frame had elapsed.

4. To view statistics for a particular port, do either of the following:
 - a. Select *Individual port overview* and then a port. The frames statistics for the selected port are displayed.
 - b. Select a frame type from the graph transmit Frames window. The statistics for the selected frame type for all of the ports is displayed.
5. To clear the graph, select *Zero all statistics counters on the entire system*.
6. Return to the Main Menu.

Displaying RMON Statistics for a Switch

To display the RMON statistics for a switch, perform the following steps:

1. From the Main Menu, select the switch whose RMON statistics you want to view.
2. From the Main Menu, select *Ethernet statistics*.

The Receive Statistics Graph in Figure 54 on page 114 is displayed.

3. Select *RMON statistics*.

The RMON Statistics Graph window is displayed. An example of the window is shown in Figure 58.

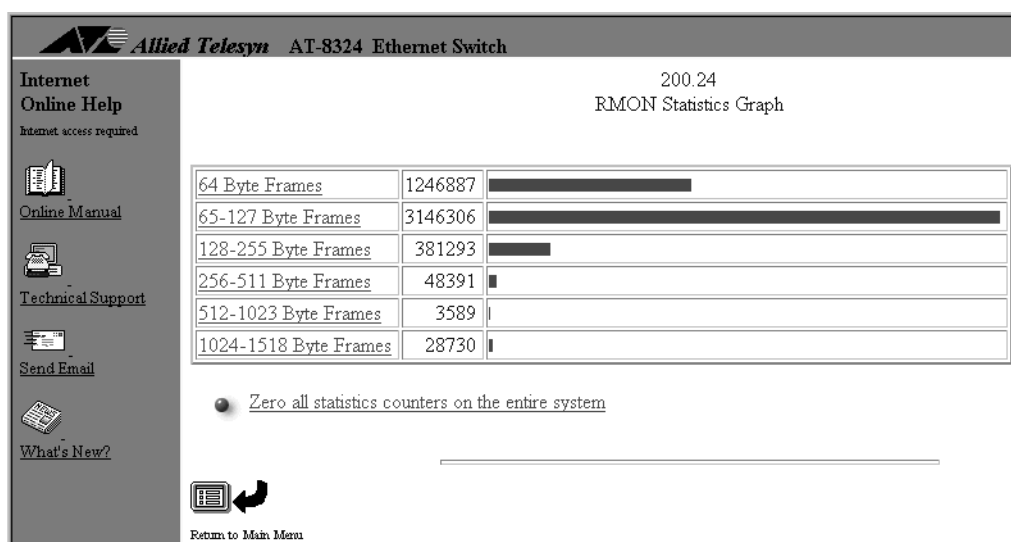


Figure 58 RMON Statistics Graph Window

4. To clear the graph, select *Zero all statistics counters from the entire system*.
5. Return to the Main Menu.

Displaying RMON Statistics for a Port

To display RMON statistics for a specific port, perform the following procedure:

1. From the Main Menu, select the switch with the port whose RMON statistics you want to view.
2. From the Main Menu, select *Ethernet statistics*.

The Receive Statistics Graph shown in Figure 54 on page 114 is displayed.

3. Select *Port RMON Statistics*.

The Omega program displays a list of the ports on the switch.

4. Select a port to display a graph similar to the following:

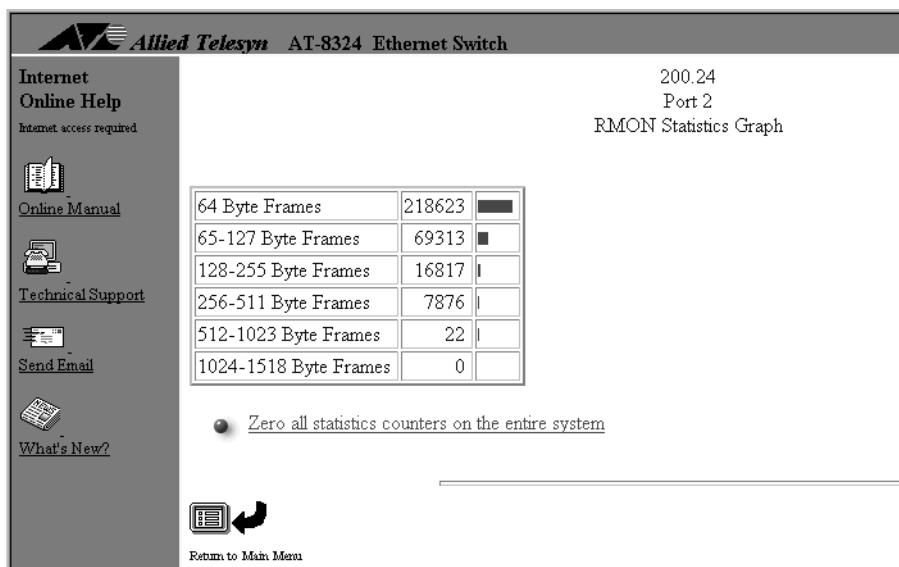


Figure 59 Sample RMON Statistics Graph for a Port

5. To clear the graph, select *Zero all statistics counters from the entire system*.
6. Return to the Main Menu.

Resetting the Statistics Counters

You reset statistics counters because:

- ☐ The counters no longer reflect the current information.

For example, disabling a port to fix a problem does not reset its counters. After the error clears and you manually re-enable the port, you may want its statistics to accumulate from a fresh start. Otherwise, the counters and graphs will reflect information associated with the error condition and the counters will continue to increment from the wrong baseline.

- ☐ As each frame type reaches the maximum of 2^{32} (over 4 billion), the statistics for that frame type resets to zero. Once this happens, the counters and graph become inaccurately skewed.

To reset switch (system) counters, perform the following procedure:

1. From the Main Menu, select the switch whose counters are to be reset to 0 (zero).
2. From the Main Menu, select *Ethernet Statistics*.
3. Select *Zero all statistics on the entire system*.

Both the receive and transmit counters and graphs are reset to 0 (zero).

Interpreting the Graphs

The statistics graphs show the types of received and transmitted frames since the last time the counters or the switch were reset. The counters and the graph dynamically increment as the switch processes frames over a period of time.

When the individual counters reach a maximum of 2^{32} (over 4 billion), they reset to zero. Because each counter resets independently, your graph may become inaccurately skewed over time; therefore, you need to reset the counters to get a new baseline on frame statistics.

The graphs help you visually monitor the proportion of good and bad frames the switch has detected. Good frames consist of filtered and forwarded broadcasts and multicasts. Bad frames are runts and long frames, or those with CRC or alignment errors. It is normal to have a number of error packets now and then. If the network seems to be "slow," this graph is one of the areas you can check to help isolate the problem.

To use the graphs as monitoring and diagnostics tools:

1. Display any of the Ethernet statistics graphs by selecting *Ethernet statistics* from the Main Menu.
2. Observe the counters and the graph.
3. Identify and then fix the problem.

Note that the problem may be external to the switch, and the statistics may just indicate an error condition somewhere on the network you need to fix. You may also need additional monitoring devices specifically designed for that purpose, such as a network analyzer, to identify the problem.

4. Select *Zero all statistics counters on the entire system* from any of the Statistics window after fixing the problem.

You need to reset counters to get a new baseline. That is because the counters and graphs still depict the information during the error condition and will continue to increment from there until you reset the counters.

Chapter 7

Configuring the Omega Interface

This chapter describes the security features of the Omega interface. These features allow you to configure the interface so as to prevent unauthorized individuals from accessing it and making changes to the configuration settings of a switch or stack. This chapter contains the following procedures:

- ❑ **Creating an Omega Password** on page 126
- ❑ **Specifying a Timeout Value** on page 128
- ❑ **Enabling and Disabling the Access Methods** on page 129

Creating an Omega Password

To prevent unauthorized individuals from accessing the Omega interface and altering a stack's configuration settings, you can assign a password to the program. Any person who starts the program will be required to enter the password, regardless of how they access the program (i.e., RS232 port, web browser, Telnet program, or SNMP management program). The default value for the Omega interface is no password.

Each stack in your network can have its own Omega password. Once an Omega password is applied to a stack, the password applies to all switches in the stack. You cannot assign individual Omega passwords to the different switches in a stack.

Note

The Omega password is not related to the download password for downloading software to a switch. For information on the download password, refer to **Chapter 7, Upgrading Switch Software and Configuration Files** on page 131.

To specify a new password for the Omega interface, perform the following procedure:

1. From the Omega Main Menu, choose *System Configuration*.

The System Configuration menu in Figure 7 on page 39 is displayed.

2. Select *Omega Options*.

The Omega Options window in Figure 60 is displayed.

Internet Online Help
Internet access required

Online Manual

Technical Support

Send Email

What's New?

Password: Enter Reset

Timeout: Enter Reset

✓ ☒ Local Omega Enabled
☐ Disable Local Omega

✓ ☒ Remote Omega Enabled
☐ No Remote Omega

✓ ☒ Web-based Omega Enabled
☐ Exclude Web-based Omega

Return to Main Menu

Figure 60 Omega Options Window

3. Enter a new password for the Omega interface in the Password field at the top of the window and press <Return>.

The password can be up to 20 characters. The password is displayed as a series of asterisks. To delete the current password but not assign a new password, enter a space in the Password field.

The password can consist of the letters A to Z in uppercase and lowercase, as well as the numbers 1 to 9. It is recommended that you avoid special characters, such as a space, asterisk (*), or exclamation point (!). Avoiding the use of special characters is particularly important if you will be managing the switch using a web browser, since browsers cannot handle special characters in program passwords.

The new password is activated immediately on the stack. You will be required to enter the password the next time you start an Omega management session.

4. Return to the Main Menu.

Specifying a Timeout Value

Specifying a timeout value is a way to prevent unauthorized individuals from using the Omega interface in the event you forget to exit the Omega interface and leave your management station unattended. By specifying a timeout value, the program will end the session if it detects that there has been no management activity after the timeout value has expired. The default for the timeout value is 5 minutes.

To enter a new timeout value, perform the following procedure:

1. From the Omega Main Menu, choose *System Configuration*.

The the System Configuration menu is displayed.

2. Select *Omega Options*.

The Omega Options window in Figure 60 on page 127 is displayed.

3. Enter a value from 0 (zero) to 65,535 (in minutes) in the Timeout field.

Entering a value of 0 means there is no timeout. The Omega interface will not end any session. A session is ended only if you end the session yourself. If you enter 0, you must always properly quit after a management session in order not to block subsequent remote sessions and software downloads to the switch.

4. Select Enter.
5. Return to the Main Menu.

The new Omega timeout value is now activated on the stack.

Enabling and Disabling the Access Methods

As explained in Chapter 1, you can access the Omega interface three different ways. You can disable one or more of the methods to enhance the security of a stack by preventing unauthorized individuals from accessing the stack and making changes to the configuration settings of the switches.

To enable or disable an Omega access method, perform the following steps:

1. From the Omega Main Menu, choose *System Configuration*.

The System Configuration menu is displayed.

2. Select *Omega Options*.

The Omega Options window in Figure 60 on page 127 is displayed.

3. Toggle the options as desired. Changes are immediately activated on the stack. The options are explained below:

Local Omega Enabled

Local Omega Disabled

These two selections allow you to control whether the Omega interface can be accessed by connecting a terminal or PC to the RS232 management port on the master switch. This is referred to as accessing the program locally. The default for this access method is enabled.

Remote Omega Enabled

Remote Omega Disabled

Accessing Omega remotely is accomplished with the Telnet program or an SNMP management program, such as HP Openview. Accessing the program remotely means you can access the program from a remote location by entering the switch's MAC address or its IP address. The default for this access method is enabled.

Web-based Omega Enabled

Web-based Omega Disabled

Web-based Omega means you can access the management menus by connecting to your switch through a web browser. This feature requires a TCP/IP network. The default is enabled.

4. Return to the Main Menu.

Chapter 8

Upgrading Switch Software and Configuration Files

This chapter contains the following procedures:

- ❑ **Upgrading the Stack Software** on page 132
- ❑ **Using Omega to Upgrade Additional Stack** on page 135
- ❑ **Uploading and Downloading System Configuration Files** on page 137

Upgrading the Stack Software

Allied Telesyn periodically updates and revises the AT-S25 software for your AT-8300 Series switches. The latest version of the software is posted on the Allied Telesyn web site for you to download onto your switches and stacks.

The file for you to download is a self-extracting compressed file. It contains several additional files. One the files is the actual software image file. It has an .IMG extension. This is the software image file that is to be used in the following upgrade directions.

You can use either by XModem or Trivial File Transfer Protocol (TFTP) to upgrade the software on a stack. Upgrading the software in a stack is accomplished by downloading the new software onto the master switch, which then automatically downloads the new software to the slave switches as a normal part of its network operations.

Upgrading the software in multiple AT-8300 stacks is simplified using the Omega interface. Rather than having to upgrade each stack manually, you need only upgrade one stack in your network and then use commands in the Omega interface to download the new software to the other stacks automatically. The Omega commands used for this are *Update Software in Another Switch* and *Broadcast Updated Software to All Systems*.

Upgrading the software in a stack involves using the Download Password. This password is required when upgrading the software except when using the XMODEM software upgrade feature. The default download password is **ATS25**. The password is case sensitive. Changing this default password to an unique password will prevent unauthorized personnel from changing the software on the switch. See **Configuring IP Parameters** on page 38 for instructions on how to change the download password.

Using XModem to Upgrade the Stack Software

Omega supports software upgrades to the switch using XModem. It is assumed that you have the required setup to support this type of file transfer.

You can upgrade the software in a stack by performing either of the following procedures:

Method 1: Using the Omega Menus

1. Start a local Omega management session.

Note

This procedure cannot be performed from a Telnet or web browser management session.)

2. From the Omega Main Menu, select *Administration* to display the Administration menu.
3. Select *XModem software update to this system*. The following prompts are displayed.

Ready to receive software upgrade via XModem.

Warning: During software update, management activity is disabled.

Do XModem update now? (Yes or No):

4. Type **Y** and wait for the following message:

The system is now ready for download.

Please start your XModem transfer.

5. Initiate the upgrade from your XModem host. The Xmodem host displays a message stating that the upgrade in progress. Be sure to wait until the switch has fully downloaded the software, performed its diagnostic tests, and reinitialized and rebooted itself before you attempt to reestablish an Omega session.

Method 2: Using the Special System Menus

1. Attach a terminal to the RS232 port on the master switch.

Note

Do not perform this procedure by attaching the terminal to an RS232 port on a slave switch. The terminal must be connected to the master switch in the stack.

2. Press the Reset button on the right side of the master switch's front panel.

3. Immediately press any key when you see the following prompt:

Hit any key to run diagnostics or to reload system software.

4. Select *XModem software update to this system*.
5. Initiate the upgrade from your XModem host.

The Xmodem host displays a message stating that the upgrade is in progress. Be sure to wait until the switch has fully downloaded the software, performed its diagnostic tests, and reinitialized and rebooted itself before you attempt to reestablish an Omega session.

Using TFTP to Upgrade Software

If you use TCP/IP protocol on your network, you can use a workstation and TFTP software to upload new software to the switch or download a copy of the current software from the switch. The switch contains the TFTP server portion of the TFTP protocol which requires that the workstation contain the TFTP client portion of the protocol.

TFTP software is available from various sources and is included in SNMPc which can be purchased through Allied Telesyn. A command line version is included in most UNIX variants and in Windows NT. Please consult the documentation or the manufacturer of the software used on the proper use of the software.

Regardless of the manufacturer, all TFTP client software will need the following information:

Host - This is the IP address of the stack to which you are uploading or downloading software.

Binary or ANSI - You will need to specify binary mode for the file transfer.

Get or Put - The Get command is used to download a copy of the software to a file on the workstation. The Put command is used to upload a new software image file to the switch.

Source file - When using the Put command to upload software to the stack, enter the path and filename of the software image that is to be uploaded. When using the Get command to download the software from a stack, enter the Download Password here.

Destination file - When using the Put command to upload software to the stack, enter the Download Password here. When using the Get command to download the software from a stack, enter the path and filename of the software image that is to be downloaded.

Using Omega to Upgrade Additional Stacks

Once you have upgrade the software on one stack in the network, you can use the Omega interface to download the new software onto the other stacks in your network.

The stack uses TFTP of the TCP/IP protocol suite to download the software between stacks. These download features will still work even if you do not use TCP/IP on your network. A stack can download software to other stacks of the same product family as long as the following conditions are met.

- ☐ If your network does not use TCP/IP, the stacks must be in the same local segment (collision domain).
- ☐ If your network uses TCP/IP and the stacks are on different subnets, the default gateway IP parameter must be properly configured in all stacks.
- ☐ All stacks must have the same Download Password as the source stacks. See the section **Configuring IP Parameters** on page 38.

Downloading Software to One Stack

To download a new version of the switch software from one stack to another stack using the Omega interface, perform the following procedure:

1. Start an Omega session with the stack that contains the new software. The session can be a local session, web-based session, or remote session.
2. From the Main Menu, select the master switch.
3. From the Main Menu, select *Administration*.
4. From the Administration menu, select, *Update software in another system*.
5. Specify the stack to upgrade using one of the following methods:
 - ☐ By its IP address, in the format **x.x.x.x**
 - ☐ By its Ethernet (or MAC) address, in the format **xxxxxxx xxxxxx** (The stacks must be on the same collision domain.)

The MAC address of a stack can be found above the master switch's RS232 management port on the front panel.

The screen immediately turns on the *Activity Monitor* screen and displays the information as the destination switch requests and then receives the software.

Repeat this procedure to download software to another stack on the network.

Downloading Software to All Switches

To download a new version of the switch software from one stack to all the other stacks using the Omega program, perform the following procedure:

1. Start an Omega session with the stack that contains the new stack software. The session can be a local session, web-based session, or a remote session.

Note

This procedure should be performed during periods of low network activity. Software broadcast updates can fail if the network is operating at a high activity rate.

2. From the Main Menu, select the master switch.
3. From the Main Menu, select *System administration*.
4. Select *Broadcast updated software to all systems*.

The master switch announces the availability of the software to the master switches in all other AT-8300 stacks; in turn, those master switches that need the upgrade respond by sending back a "request" message.

The screen immediately turns on the Activity Monitor screen and displays the information as the master switches on the network request and then receive the software.

Note

You cannot undo this command once it is executed.

You may go to menus without interrupting the software download.

If you have many switches requesting the download, not all of them may receive it especially if the network is busy. Repeat the procedure to ensure all switches receive the software upgrade.

Note

Switches with different download passwords will not receive the software download.

Uploading and Downloading System Configuration Files

The switch configuration information can also be downloaded and saved to a file on a workstation. This file can then be used to restore the configuration information to the same switch or can be uploaded to other switches of the same family that need to be configured identically.

TFTP is used to download and upload the switch configuration information. Please refer to the section **Using TFTP to Upgrade Software** on page 134 for requirements and instructions for using TFTP.

The only difference is you must now use the Config Download Password to access the switch configuration information. By default this Config Download Password is set to **config** and is case sensitive. Changing this default password to a unique password will prevent unauthorized personnel from copying or uploading an unauthorized configuration to the switch. See the section **Configuring IP Parameters** on page 38 for instructions on how to change the download password.

The basic TFTP parameters for downloading and uploading the switch configuration information would be as follows.

Host - This is the IP address of the switch that you are uploading or downloading the configuration information to.

Binary or ANSI - You need to specify binary mode for the file transfer.

Get or Put - The Get command is used to download a copy of the switch configuration information to a file on the workstation. The Put command is used to upload an existing switch configuration file to the switch.

Source file - When using the Put command to upload a configuration file to the switch, enter the path and filename of the configuration file that is to be uploaded. When using the Get command to download the software from a switch, enter the Config Download Password here.

Destination file - When using the Put command to upload a configuration file to the switch, enter the Config Download Password here. When using the Get command to download the configuration information from a switch, enter the path and filename of the file that you want to save the information to.

Note

The switch configuration file created with these procedures cannot be edited.

Appendix A

Introduction to Virtual LANs

A virtual LAN (VLAN) is a group of end nodes that function as if they are a part of the same LAN segment. A VLAN can consist of end nodes located in one specific area of a network or of end nodes that are widely dispersed. This flexibility allows you to form logical workgroups of end nodes located anywhere on your network.

A VLAN constitutes a broadcast domain. A VLAN restricts the transmission of broadcasts only to the end nodes that are members of the same VLAN. Members of a VLAN can communicate directly with other members of the same VLAN. If an end node needs to communicate with a member of another VLAN, a routing device or a Layer 3 switch is required.

There are a number of advantages to VLANs:

- ❑ Improve network performance — Grouping end nodes with related functions in the same virtual LAN can reduce the amount of data traffic on each segment.
- ❑ Improve network security — When networking devices, such as workstations and servers, are grouped into a VLAN, data is exchanged only between those members of the group. This can help to limit unauthorized access to restricted data and network devices.
- ❑ Simplify network management — Moving network devices between LAN segments can be accomplished through software management, without having to move the devices physically or having to rewire connections to switches in the wiring closet.

The AT-8324 and AT-8316F Series Switches support three types of VLANs:

- ☐ Port-based VLANs
- ☐ Tagged VLANs
- ☐ Basic VLAN Mode

All three types of VLANs are described in the following sections.

Port-based VLAN

A port-based VLAN is a group of ports on an AT-8324 or AT-8316F Series switch that have been grouped together to form a logical Ethernet segment. A port-based VLAN can have as many or as few ports as needed. The VLAN can include ports from just one switch in an AT-8300 stack, or it can include ports from multiple switches in a stack. A port-based VLAN can even span different stacks or switches (including AT-8224XL and AT-8216F Series switches).

Parts of a Port-based VLAN

The parts that make up a port-based VLAN are:

- ☐ VLAN name
- ☐ VLAN Identifier
- ☐ Port VLAN Identifier
- ☐ Untagged ports

VLAN Name

To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices to be members of the VLAN. Examples include Sales, Production, or Engineering.

VLAN Identifier

Each VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of the ports located on one physical AT-8300 Series stack in your network, you would assign it a VID unique from all other VLANs in your network. If a VLAN spans multiple stacks or switches, then the VID for the VLAN on each stack or switch will be the same. In this manner, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN itself spans multiple switches. For example, if you had a port-based VLAN titled Marketing that spanned three switches, you would assign the Marketing VLAN on each of the switches the same VID.

You can assign this number manually or allow the AT-S25 software to do it automatically. The range of the VID varies depending on whether IGMP snooping is activated on an AT-8300 Series stack. If IGMP snooping is not activated, the VID range is from 2 to 4096. If IGMP snooping is activated, the range is 2 to 2047. You should take this into account when planning your VLANs and assigning VID values. If IGMP snooping is not activated on a stack but that you might activate it at a later time, it is recommended that you assign VLANs VID values in the range of 2 through 2047. This could save you from having to reconfigure your VLAN VID assignments should you later activate IGMP snooping.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, assume that you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID 5. Consequently, the PVID for each port in the VLAN would need to be assigned the value 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the AT-S25 management software performs this task automatically. The software automatically assigns a PVID to a port when the port is assigned to a port-based VLAN. A port's PVID assigned by the management software is the same as the VID of the VLAN to which the port is made a member.

Untagged Ports

Naturally, you also need to specify which ports on a switch or stack are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the port as *untagged frames*. The names originate from the fact that the frames received on a port will not contain any tagged information that indicates VLAN membership, and that VLAN membership is determined by the port's PVID. (As explained in **Tagged VLAN** on page 147, there is another type of VLAN where VLAN membership is determined by information within the frames themselves, rather than by a port's PVID.)

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

General Rules to Creating a Port-based VLAN

Below is a summary of the rules to observe when creating a port-based VLAN.

- ☐ Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiples switches or stacks, each part of the VLAN on the different switches or stacks must be assigned the same VID.
- ☐ An port can be an untagged member of only one port-based VLAN at a time.
- ☐ When creating a VLAN in an AT-8300 stack, you create the VLAN only once. You do not create the VLAN separately on each switch in a stack. Once you have created the VLAN, you can assign it ports from any or all of the switches in the stack.
- ☐ Each port must be assigned a PVID. This value must be the same for all ports in a port-based VLAN and must match the VLAN's VID. This function is performed automatically by the AT-S25 management software.
- ☐ A port-based VLAN that spans multiple switches or stacks will require a port on each switch or stack where the VLAN is located to function as an interconnection between the switches where the various parts of the VLAN reside. This is illustrated in the section **Port-based VLAN Example** on page 144.
- ☐ If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch will be required to interconnect the VLANs.

Port-based VLAN Example

Figure 61 is an example of two port-based VLANs that span an AT-8300 Series stack and one AT-8224XL Switch.

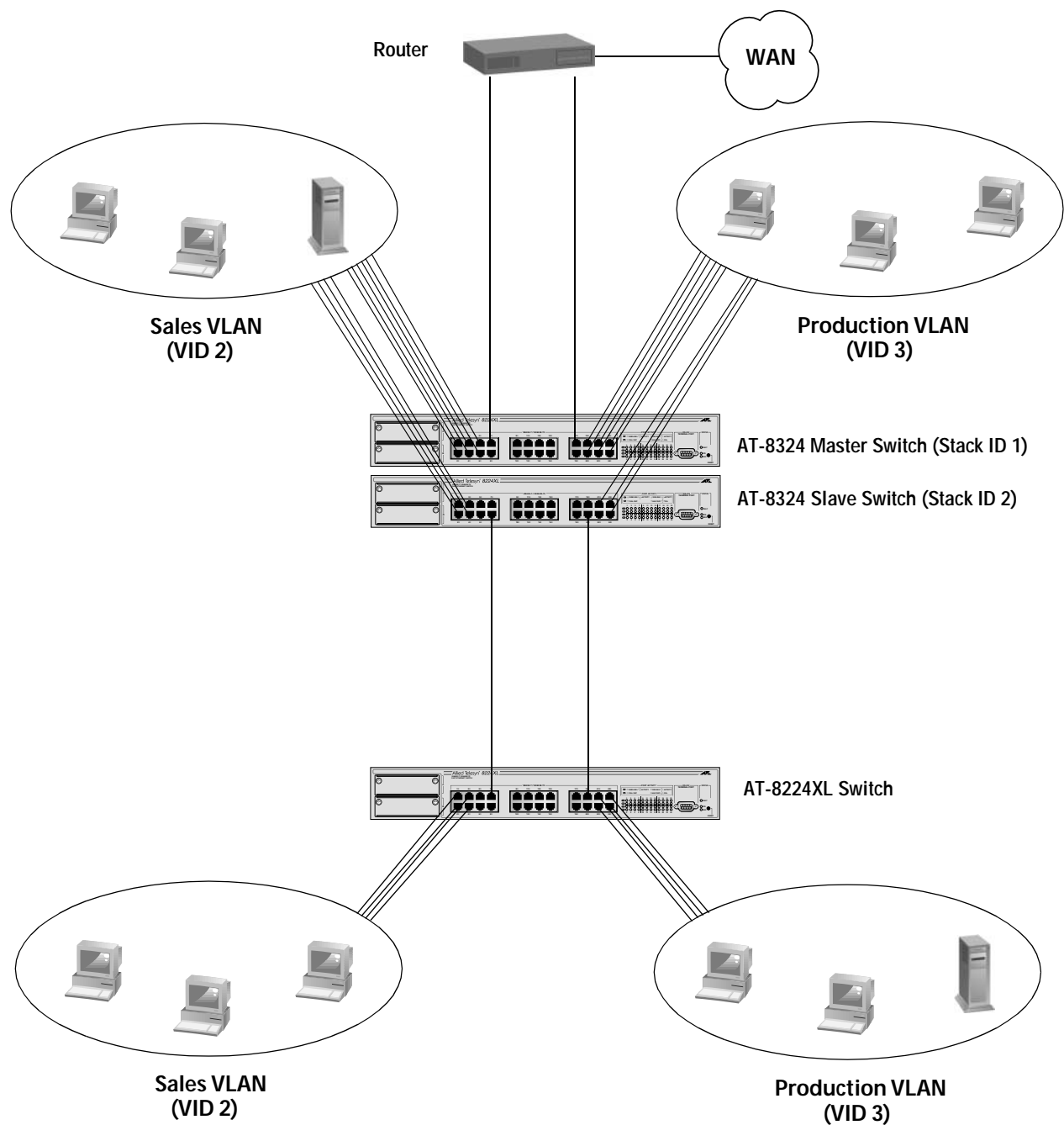


Figure 61 Port-based VLAN Example

The table below lists the ports assignments for the Sales and Production VLANs:

Table 8-1 Port Assignments of the Port-based VLAN Example

	Sales VLAN (VID 2)	Production VLAN (VID 3)
AT-8300 Series Stack		
AT-8324 Switch (master)	Ports 1 - 7 (PVID 2)	Ports 17, 19 - 24 (PVID 3)
AT-8324 Switch (slave)	Ports 1 - 4, 8 (PVID 2)	Ports 20, 21, 23, 24 (PVID 3)
AT-8224XL Switch	Ports 1 - 4, 7 (PVID 2)	Ports 19, 21 - 24 (PVID 3)

Each VLAN is briefly summarized below:

- ❑ **Sales VLAN** — This VLAN has been assigned a VID of 2 and the ports, correspondingly, have been automatically assigned a PVID also of 2. This VLAN spans both the AT-8300 Series stack and the AT-8224XL Switch. Ports 1 to 6 on the master AT-8324 Switch and ports 1 to 4 on the slave switch are connected to workstations and a server. Port 7 on the master switch is connected to the router, which allows the Sales VLAN to communicate with the Production VLAN and also to the WAN. Port 8 on the slave switch is functioning as a direct link to the second part of the Sales VLAN, located on the AT-8224XL Switch.
- ❑ **Production VLAN** — This VLAN has been assigned a VID of 3 and the ports a PVID of 3. Ports 19 to 24 on the master AT-8324 Switch and ports 21, 23, and 24 on the slave switch are connected to workstations. Port 17 on the master switch is connected to a router for interconnection to the Sales VLAN and the WAN, and port 20 on the slave switch is connected to the AT-8224XL Switch to interconnect the two parts of the Production VLAN.

Drawbacks to Port-based VLANs

There are several drawbacks to port-based VLANs:

- ❑ It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router must be added to the network to provide a means for interconnecting the port-based VLANs.
- ❑ The introduction of a router into your network could create security issues from unauthorized access to your network.
- ❑ A VLAN that spans several switches will require a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches would require one port on each switch just to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports can end up being used ineffectively just to interconnect the various VLANs.

Tagged VLAN

The second type of VLAN is referred to as a *tagged VLAN*. With a tagged VLAN, VLAN membership is determined by information within the frames that are received on a port. This contrasts to a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within the frames is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). As explained earlier in this chapter in **VLAN Identifier** on page 141, this number uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID. A port to receive or transmit tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The main benefit of a tagged VLAN is that the tagged ports within the VLAN can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network and interconnecting VLANs that span multiple switches. For example, a server can be configured to accept and return packets from many different VLANs simultaneously. Additionally, where multiple VLANs span across switches, you can use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame will be accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame will be discarded.

Parts of a Tagged VLAN

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are:

- ☐ VLAN Name
- ☐ VLAN Identifier
- ☐ Port VLAN Identifier
- ☐ Tagged and Untagged Ports

Each item is described in the following sections.

Note

For explanations of VLAN name and VLAN identifier, refer back to **VLAN Name** and **VLAN Identifier** on page 141.

Port VLAN Identifier

As explained earlier in this appendix in the discussion on port-based VLANs, the AT-S25 software automatically assigns a PVID to each port when a port is made a member of a VLAN. The PVID is always identical to the VLAN's VID, and that in a port-based VLAN packets are forwarded based on the PVID.

But since a tagged port determines VLAN membership by examining the tagged header within the frames that it receives, there would seem to be no need for a PVID. But actually there is. If a tagged port receives an untagged frame (that is, a frame without any tagged information), the port will forward the frame based on the ports PVID. But this is only in the case where untagged frames arrive on tagged ports. Otherwise, the PVID of a port is ignored on a tagged port.

Tagged and Untagged Ports

You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, it will usually be a combination of both untagged ports and tagged ports. You will specify which ports will be tagged and which untagged when you create the VLAN with the AT-S25 management software.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs, simultaneously.

General Rules to Creating a Tagged VLAN

Below is a summary of the rules to observe when creating a tagged VLAN.

- ☐ Each tagged VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches or stacks, each part of the VLAN on the different switches or stacks must be assigned the same VID.
- ☐ An untagged port can be an untagged member of only one VLAN at a time.
- ☐ A tagged port can be a member of multiple tagged VLANs.
- ☐ When creating a tagged VLAN in an AT-8300 stack, you create the VLAN only once. You do not create the VLAN separately on each switch in a stack. Once you have created a VLAN, you can assign it ports from any or all of the switches in the stack.
- ☐ Each port must be assigned a PVID. This value must be the same for all ports in a port-based VLAN and must match the VLAN's VID. This function is performed automatically by the AT-S25 management software.

Tagged VLAN Example

Figure 62 is an example of a network that uses tagged ports in two tagged VLANs to share network devices.

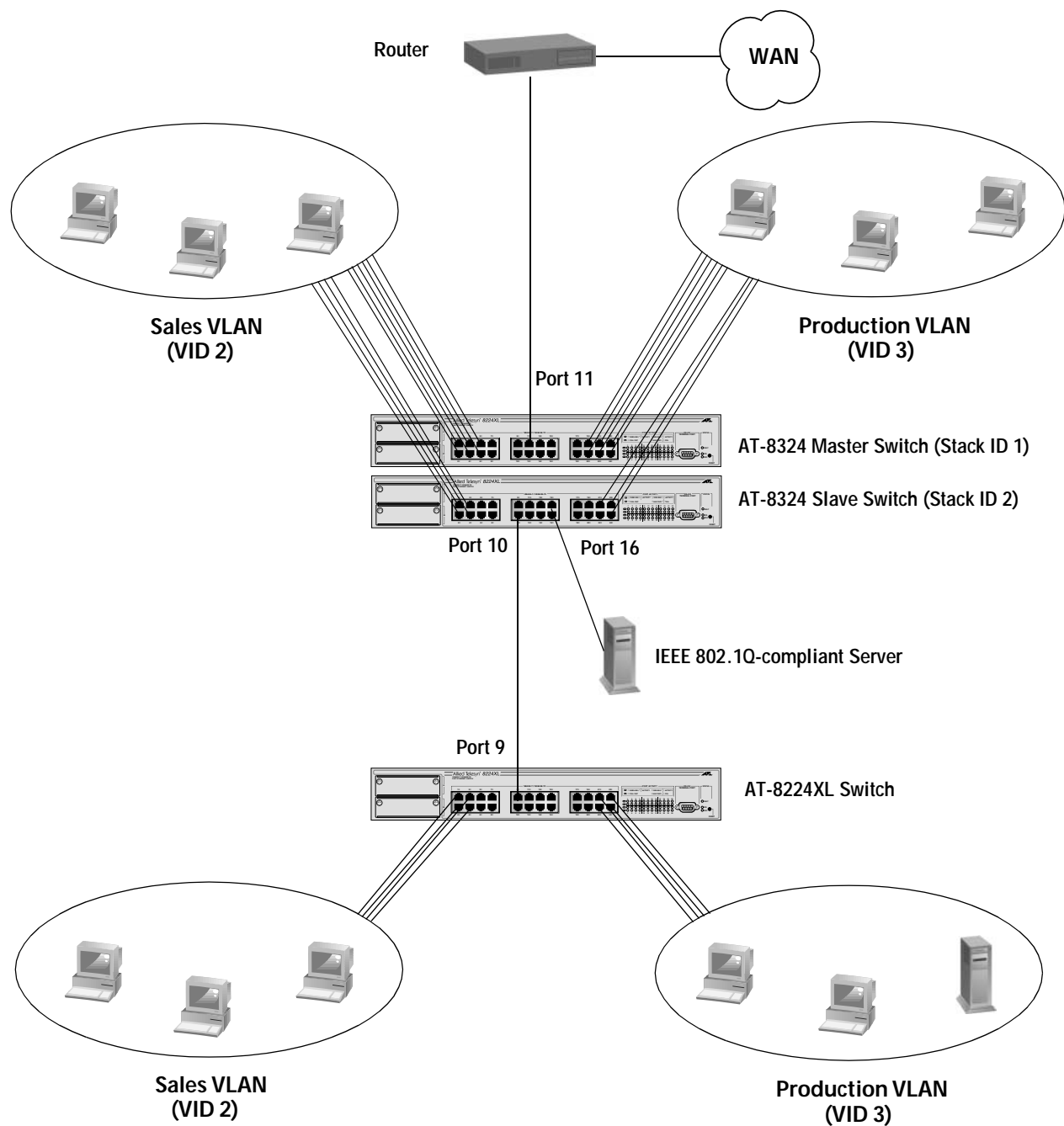


Figure 62 Tagged VLAN Example

The port assignments for the VLANs are as follows:

	Sales VLAN (VID 2)		Production VLAN (VID 3)	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-8300 Series Stack				
AT-8324 Switch (Master)	1 to 6 (PVID 2)	11	19 - 24 (PVID 3)	11
AT-8324 Switch (Slave)	1 - 4 (PVID 2)	10, 16	22 - 24 (PVID 3)	10, 16
AT-8224XL Switch	1 - 4 (PVID 2)	9	21 - 24 (PVID 3)	9

This configuration is similar to the port-based VLAN example earlier in this appendix, but untagged ports have replaced several connections. The changes are noted below:

- ❑ Uplink to the AT-8224XL switch - In the earlier port-based VLAN example, each VLAN in the AT-8300 stack had a dedicated connection to its corresponding VLAN in the AT-8224XL Switch. These connections have been replaced with one connection. Port 10 on the AT-8324 slave switch has been made a tagged member of both VLANs, as has port 9 on the AT-8224XL switch. The connection between the ports now carries traffic for both VLANs. However, frame traffic is restricted to its respective VLAN member ports.
- ❑ Uplink to an IEEE 802.1Q-compliant server - Port 16 on the AT-8324 slave switch has been connected to an IEEE 802.1Q-compliant server, meaning the device is capable of handling tagged frames. By designating it as a tagged port of both the Sales and Production VLANs, end-nodes from either VLAN can access the resource without having to pass through a router.
- ❑ Uplink to an IEEE 802.1Q-compliant router - Port 11 on the AT-8324 master switch has been connected to a router and has been made a tagged member of both VLANs. Access to the WAN is now possible for both VLANs over the one connection.

Basic VLAN Mode

The third type of VLAN system support by the AT-8316F Series and AT-8324 Switches is referred to as the Basic VLAN Mode. When the Basic VLAN Mode is activated, the switch or stack forwards frames based only on MAC addresses. All VLAN information, including PVIDs assigned to ports and VLAN tags in tagged frames, are ignored. Tagged frames are analyzed only for priority level.

Packets are passed through the switch unchanged. Tagged and untagged frames egress the switch the same as they entered, either tagged or untagged, regardless of the type of port on which the frame is received or transmitted.

You cannot create or modify VLANs when the Basic VLAN Mode is activated, and the *Virtual LAN/QOS* selection is removed from the Omega Main Menu. The configurations of any pre-existing VLANs are retained in the event you later disabled Basic VLAN Mode, but the VLAN configurations are not used.

For instructions on how to enable or disable the Basic VLAN Mode, refer to **Activating or Deactivating the Basic VLAN Mode** on page 107 in **Chapter 5**.

Appendix B

AT-S25 Default Settings

This appendix lists the AT-S25 Version 1.4 factory default settings.

Settings	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
Domain Name Server	None
Default Domain Name	None
Download Password (AT-S25 Image File)	ATS25
Config Download Password (Configuration File)	config
IGMP Snooping	Disabled
System Name	None
MAC Aging Time	300 seconds
Domain Name	None
Community Strings	
Get Community String	public
Set Community String	private
Trap Community String	public
Spanning Tree Protocol	
Status	Disabled
Bridge Priority	32768
Bridge Max Age Time	20
Bridge Hello Time	2
Bridge Forwarding Delay	15

Settings	Default
Omega	
Omega Password	No password
Omega Time Out Value	5 minutes
Local Access	Enabled
Remote Access (Telnet or SNMP)	Enabled
Web-based Access	Enabled
AT-8324 Twisted Pair Ports	
Status	Enabled
Duplex Mode	Auto-negotiation
Speed	Auto-negotiation
Backpressure	Disabled
Flow Control	Disabled
Broadcast Packets	Forwarded
Security	Automatic
AT-8316F Fiber Optic Ports	
Status	Enabled
Duplex Mode	Full-duplex
Speed	100 Mbps
Security	Automatic
VLANs	
Default VLAN Name	Default VLAN (all ports)
VID	1
RS232 Port	
Configuration	VT-100-compatible / ANSI
Data Bits	8
Stop Bits	1
Parity	None
Duplex Mode	Full-duplex
Data Rate	9600 bps

Appendix C

Spanning Tree Protocol Concepts

This appendix provides a brief explanation of the Spanning Tree Protocol (STP) as implemented by Allied Telesyn on the AT-8300 Series Fast Ethernet Switches.

For detailed information on the operation of the Spanning Tree Protocol, consult Section 4 of IEEE Std 802.1D, ISO/IEC 10038: 1993.

The AT-8300 switches, which run the AT-S25 software, implement the IEEE 802.1D Spanning Tree Protocol. The STP provides a network with robustness and allows network administrators to easily change their network topology. Its implementation reduces complex network topologies (networks with multiple paths between source and destination nodes) to a single active topology. This technique guarantees that loops do not occur between source and destination nodes of the network. Loops are eliminated by placing some of the redundant ports in a “blocking” state, in which they do not forward packets but continue to execute the protocol. If the network topology changes, for example by the failure, removal, or addition of an active network node, a “blocked” port may be included in the new active topology and begin forwarding frames.

Spanning Tree Protocol Features

The switches implement the following STP features:

- ☐ Compensate automatically for the failure, removal, or addition of any bridge in an active data path.
- ☐ Achieve port changes in short time intervals, which establishes a stable active topology quickly with a minimum of network disturbance.
- ☐ Use a minimum amount of communications bandwidth to accomplish the operation of the STP.
- ☐ Reconfigure the active topology in a manner which is transparent to stations transmitting and receiving data packets.
- ☐ Manage the topology in a consistent and reproducible manner through the use of STP parameters.

Spanning Tree Protocol Parameters

Several configuration parameters control the operation of the Spanning Tree Protocol. Table 7 describes the parameters and lists each parameter's default settings for the switch.

Table 7 Spanning Tree Protocol Parameters

Parameter and Description	Default
Bridge Group Address Unique MAC group address, recognized by all bridges in the network	N/A
Bridge Identifier Identifier for each bridge, consisting of two parts: a 16-bit bridge priority and a 48-bit network adapter address. Ports are numbered in absolute numbers; from 1- <i>n</i> for a multi-port switch including optional expansion ports, if any. The network adapter address is the same address as the first port of the bridge.	32768 (bridge priority)
Port Priority	128
Port Cost The spanning tree algorithm calculates and ensures that an active topology generates minimal path costs.	100 for 10 Mbps ports 10 for 100 Mbps ports

Spanning Tree Protocol Operation

When STP is enabled for the first time, or when the network topology changes due to a failure, the addition, or removal of a component, the spanning tree algorithm automatically sets up the active topology of the current network.

Communication Between Bridges

Periodically, all devices running STP on a network transmit packets to each other through the Bridge Group Address which all bridges share. When a bridge receives a packet sent to the Bridge Group Address, the bridge's STP processes the packet. The packet is ignored by application software and other LAN segments. Bridges communicate between each other in order to determine the **root bridge**.

Selecting a Root Bridge and Designated Bridges

During communication between bridges, one bridge is determined to have the lowest bridge identifier. This bridge becomes the root bridge.

After the root bridge has been selected, each LAN segment looks for the bridge that has the lowest cost relative to the root bridge. These bridges become designated bridges.

Selecting Designated Ports

Each designated bridge selects a **designated port**. This port is responsible for forwarding packets to the root bridge.

Handling Duplicate Paths

When the active topology of the network is determined, all packets between any two nodes in the network use only one path. Where a duplicate path exists, the non-designated port is put into a blocking state.

Remapping Network Topology

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports.

The blocked ports do not forward packets immediately. They first pass through two states, listening and learning, to verify that they may begin forwarding. A port remains in each of these two states for the time defined by the Forwarding Delay parameter. This algorithm ensures that no temporary loops exist in the active network topology and is a safeguard against packet forwarding during a network topology change period.

Appendix D

Supported Platforms

Table 8 lists the Allied Telesyn Fast Ethernet switches that are supported by the AT-S25 Version 1.2 software.

Table 8 Switch Models

Model ¹	Number of Ports	Type of Ports	Type of Connector	Maximum Distance ²
AT-8324	24	10/100Base-TX	RJ-45	100 m (328 ft)
AT-8316F/MT	16	100Base-FX	MT-RJ	2 km (1.25 mi)
AT-8316F/VF	16	100Base-FX	VF-45	2 km (1.25 mi)
AT-8316F/SC	16	100Base-FX	SC	2 km (1.25 mi)

1. All models include two expansion slots.

2. The maximum distance may be less depending on the duplex mode of the end nodes and the type of cabling used with the module.

Table 9 lists the optional expansion modules supported by the software.

Table 9 Optional Expansion Modules

Model	Number of Ports	Type of Ports	Type of Connector	Maximum Distance ¹
AT-A14	1	100/1000Base-T	RJ-45	100 m (328ft)
AT-A15/SX	1	1000Base-SX	SC	550 m (1,804 ft)
AT-A15/LX	1	1000Base-LX	SC	10 km (6.2 mi)
AT-A16	2	100Base-FX	VF-45	2 km (1.25 mi)
AT-A17	2	100Base-FX	SC	2 km (1.25 mi)

Table 9 Optional Expansion Modules

Model	Number of Ports	Type of Ports	Type of Connector	Maximum Distance¹
AT-A18	4	10/100Base-TX	RJ-45	100 m (328 ft)
AT-A19	2	100Base-FX	MT-RJ	2 km (1.25 mi)
AT-A22/SX	1	1000Base-SX	SC	550 m (1,804 ft)
AT-A22/LX	1	1000Base-LX	SC	10 km (6.2 mi)
AT-A24/SX	1	1000Base-SX	MT-RJ	550 m (1,804 ft)
AT-A24/LX	1	1000Base-LX	MT-RJ	10 km (6.2 mi)

1. The maximum distance may be less depending on the duplex mode of the end nodes and the type of cabling used with the module.

Index

(Items in *italic* are menu selections.)

A

- Activity monitor*, 60
- activity monitor, 60
- Add MAC Address*, 88
- Add new table entry*, 99
- adding static MAC addresses, 88
- addresses
 - IP, 41
 - MAC, 82
 - multicast, 92
 - static, 87
- Administration*, 32
- aging time
 - bridge, 47
 - MAC address table, 86
- alignment errors, 115
- All static MAC addresses*, 87
- ANSI terminal, 21
- Assign Management Port to VLAN*, 110
- Assign Port Priority*, 109
- AT-8316F Ethernet switch
 - port groups, 71
- AT-8324 Ethernet switch
 - port groups, 71
 - port speed, setting, 68
- AT-S25 software
 - reassigning default values, 53
 - upgrading, 132, 135
 - version number, 58
- audience, this guide, 8

- Automatic level, port security, 79
- auto-negotiation, 67

B

- backpressure, 68
- Basic VLAN Mode, 107, 152
- baud rate, 57
- bookmarks, 28
- Bootp, 38
- BPDU, *see* bridge protocol data unit
- bridge group address, 157
- bridge identifier, 157
- bridge priority, 47
- bridge protocol data unit (BPDU), 47
- Bridging*, 34
- broadcast packets, 68
- broadcast statistics, 115, 119
- Broadcast updated software to all systems*, 136
- browser tools, 28
- By port MAC addresses*, 84

C

- Clear static MAC table*, 91
- clearing the static MAC address table, 91
- community strings, SNMP, 42
- Config Download password, 42
- configuration files, uploading or downloading, 137
- configuring
 - multicast addresses, 92
 - port parameters, 66
 - priority queueing, 108

- STP parameters, 46
- STP port parameters, 43
- switch IP parameters, 38
- Connect to remote system*, 31
- connecting to remote stack, 31
- conventions, used in this guide, 10
- cost, 46
- CPU management port, 110
- CRC errors, 115
- creating a VLAN, 98

D

- data bits, 56
- data rate, 57
- DEC VT100 terminal, 21
- Default Aging Time*, 86
- default domain name, 41
- default settings
 - reassigning stack default values, 53
- Default VLAN, 97
- Delete MAC Address*, 94
- deleting
 - multicast addresses, 94
 - port trunk, 75
 - static MAC addresses, 90
 - VLAN, 106
- Destination Port*, 77
- DHCP server, 38
- Diagnostics*, 58
- diagnostics, running, 58
- Disable Spanning Tree for all Ports*, 45
- disabling port mirroring, 78
- displaying
 - MAC address table by address, 85
 - MAC address table, 83
 - MAC addresses by port, 84
 - port status, 64
 - received frame statistics, 114
 - RMON statistics, 120, 121
 - transmitted frame statistics, 118
- documentation set, list, 11
- domain name server, 41
- download password, 41, 132
- downloading AT-S25 software
 - all switches, 136
 - one stack, 135
- downloading configuration files, 137

E

- emulation, terminal, 21
- Enable Spanning Tree for all Ports*, 45
- enabling port mirroring, 76
- Enter button, 27
- Ethernet Statistics*, 114
- Ethernet statistics*, 32

F

- filtered frames, 115
- flow control, 68
- forwarding delay, 48
- fragments, 115
- full-duplex, 57, 67

G

- gateway address, 41
- generic terminal, 22
- Get Port From MAC Address*, 85
- global configuration, 68
- graphical switch, 26
- graphs, statistics
 - received frames, by frame type, 116
 - received frames, port level, 116
 - transmitted frames, switch level, 118
 - use as diagnostic tool, 122
- guidelines, port trunking, 70

H

- half-duplex, 57, 67
- Hello time, 48

I

- IEEE 802.1d standard, 48
- Individual port overview*, 116, 119
- Internet Group Management Protocol (IGMP)
 - support, 49
- Internet Group Management Protocol, 49
- IP address, 41
- IP Parameters*, 40
- IP parameters, configuring, 38

- L**
- late collisions, 119
 - local Omega session
 - enabling or disabling, 129
 - quitting, 23
 - starting, 19
 - long frame, 115
- M**
- MAC address table
 - aging time, configuring, 86
 - defined, 82
 - displaying, 83
 - displaying by MAC address, 85
 - displaying by port, 84
 - MAC address, 58
 - main menu
 - local session, 20
 - web browser session, 26
 - management port. See CPU management port
 - manager address, 41
 - master switch
 - configuring the RS232 port, 55
 - defined, 21, 27
 - max age time parameter, 47
 - menu selections
 - Activity monitor*, 60
 - Add MAC Address*, 88
 - Add new table entry*, 99
 - Administration*, 32
 - All static MAC addresses*, 87
 - Assign Management Port to VLAN*, 110
 - Assign Port Priority*, 109
 - Broadcast updated software to all systems*, 136
 - By port MAC addresses*, 84
 - Clear static MAC table*, 91
 - Connect to remote system*, 31
 - Default Aging Time*, 86
 - Delete MAC Address*, 94
 - Diagnostics*, 58
 - Ethernet Statistics*, 114
 - Ethernet statistics*, 32
 - Get Port From MAC Address*, 85
 - Individual port overview*, 116, 119
 - IP Parameters*, 40
 - menu tree, 32
 - Multicast addresses*, 92
 - Omega options*, 126, 128, 129
 - Per port static MAC addresses*, 88, 90
 - Ping a remote system*, 61
 - Port Configuration and Statistics*, 64, 66
 - Port RMON statistics*, 121
 - Port spanning tree configuration*, 44
 - Port Status and Configuration*, 32
 - Port trunking*, 73, 75
 - Reset and restart the system*, 52
 - RMON statistics*, 120
 - Security/Source Address Table*, 79
 - Show all MAC addresses*, 83
 - Spanning tree parameters*, 46
 - Switch-mode Selection*, 107
 - System Configuration*, 33, 55
 - System Name*, 50
 - Traffic/Port Mirroring*, 34, 76, 78
 - Transmit Statistics*, 118
 - Update software in another system*, 135
 - Virtual LAN definitions*, 99, 105, 106
 - XModem software update to this system*, 134
 - menu tree, 32
 - modifying a VLAN, 105
 - multicast addresses
 - changing, 94
 - configuring, 92
 - defined, 92
 - deleting, 94
 - Multicast addresses*, 92
 - multicast statistics, 115, 119
- N**
- naming a stack, 50
- O**
- Omega interface
 - main menu, 20, 26
 - menu tree, 32
 - security, 125
 - Omega options*, 126, 128, 129
 - Omega session
 - bookmarks, 28
 - local, 19
 - web browser, 24
 - Online Manual web link, 28
 - organization, this guide, 9

P

- parity, 57
- partitioning a port, 67
- password
 - Config Download, 42, 137
 - download, 41
 - Omega interface, 126
- Per port static MAC addresses*, 88, 90
- Ping a remote system*, 61
- ping command, 61
- Port Configuration and Statistics*, 64, 66
- port cost, 157
- port groups, 71
- port mirroring
 - defined, 76
 - enabling, 76
- port mirroring, disabling, 78
- port name, 69
- port priority, 157
- Port RMON statistics*, 121
- port security, 79
- Port spanning tree configuration*, 44
- Port Status and Configuration*, 32
- port status, 64
- port trunking
 - creating, 73
 - defined, 70
 - deleting, 75
 - guidelines, 70
- Port trunking*, 73, 75
- port VLAN identifier (PVID), 148
- port-based VLAN
 - creating, 98, 101
 - defined, 141
 - deleting, 106
 - modifying, 105
- ports
 - configuring parameters, 66
 - configuring STP parameters, 46
 - displaying RMON statistics, 121
- priority queueing, VLANs, 108
- priority, 46
- purpose, this guide, 8, 9

Q

- Quit*, 31
- quitting
 - local Omega session, 23
 - Telnet Omega session, 29
 - web browser Omega session, 28

R

- received frame statistics, 114
- received good frames, 115
- remote Omega session
 - enabling or disabling, 129
- remote stack, connecting to, 31
- Reset and restart the system*, 52
- Reset button, 27
- resetting a stack, 51
- resetting statistics counters, 122
- RMON statistics, 120, 121
- RMON statistics*, 120
- root bridge, 47, 158
- root port, 158
- RS232 port
 - configuring, 55
 - default settings, 19, 53
- running diagnostics, 58

S

- Secure level, port security, 80
- security, Omega interface, 125
- Security/Source Address Table*, 79
- Send Email web link, 28
- Show all MAC addresses*, 83
- single collision, 119
- SNMP community strings, 42
- snooping, 49
- Source Module*, 77
- Source Port*, 77
- Spanning tree parameters*, 46
- spanning tree protocol
 - concepts, 155
 - configuring parameters, 46
 - configuring port parameters, 43
 - defined, 43
- stack
 - connecting to remote, 31
 - MAC address, 58
 - naming, 50

- reassigning default settings, 53
- resetting, 51
- upgrading AT-S25 software, 132
- Stack ID setting, 20, 27
- starting Omega session
 - local, 19
 - web browser, 24
- static MAC address table
 - adding addresses, 88
 - clearing, 91
 - defined, 87
 - deleting addresses, 90
 - displaying, 87
- statistics
 - graphs interpretation, 122
 - received frames, 114
 - resetting counters, 122
 - RMON, 120, 121
 - transmitted frames, 118
 - transmitted frames, description, 119
- stop bits, 57
- STP, *see* spanning tree protocol
- subnet mask, 41
- switch
 - configuring IP parameters, 38
- Switch-mode Selection*, 107
- System Configuration*, 33, 55
- System Name*, 50

T

- tagged ports, 148
- tagged VLAN
 - creating, 98, 103
 - defined, 147
 - deleting, 106
 - example, 150
 - modifying, 105
- Technical Support web link, 28
- Telnet management session
 - starting, 29
- terminal emulation, 21
- terminal interface, 21
- TFTP, to upgrade AT-S25 software, 134
- timeout value, 128
- total good transmits, 119
- Traffic/Port Mirroring*, 34, 76, 78
- Transmit Statistics*, 118

- transmitted frame statistics, 118

U

- undersized frames, 115
- untagged ports, 148
- Update software in another system*, 135
- upgrading AT-S25 software
 - using Omega, 135
 - using TFTP, 134
 - using XModem, 133
- uploading configuration files, 137

V

- Virtual LAN definitions*, 99, 105, 106
- Virtual LANs/QoS*, 34
- VLAN identifier (VID), 100, 141
- VLANs. *See* Basic VLAN Mode, Tagged VLANs, and Untagged VLANs

W

- web browser Omega session
 - enabling or disabling, 129
 - quitting, 28
 - starting, 24
 - web links, 28
- What's New web link, 28

X

- XModem software update to this system*, 133, 134
- XModem, to upgrade AT-S25 software, 133

